ADVOCATE GUIDE: RING SECURITY DEVICES

GUIDE OVERVIEW

If you are working with a survivor who owns or is contemplating installing a Ring device, this resource is intended to supplement the **Ring Survivor Safety Guide** and provide information about risks and benefits, approaches to addressing common issues and troubleshooting tips.

At the end of this guide is a safety plan template that will be helpful to fill out together with the survivor, either before they set up their device or after they already have it installed. While specific to some Ring settings, the information in this guide may be applicable to other home security devices as well.

Feel uncomfortable discussing technology? You can learn more about common tech privacy and confidentiality considerations and resources at NNEDV's Technology Safety website here.

RING DOORBELL

ABOUT RING DEVICES

Ring Video Doorbell:
There are both wired and battery-operated versions which use the home's WiFi network. From the Ring app or their online account, survivors can receive motion alerts, view a live video feed and speak to people via the device. More details can be found here.

Stick Up Cam:
This is a security camera that can be placed anywhere (outside or inside). Like the doorbell, survivors can receive motion alerts, view a live video feed and speak to people via the device from the Ring app. More details can be found here.

While we focus on these two devices, Ring has many other devices available. Read more about them at Ring.com.

RING SET-UP

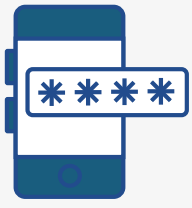
Ring devices are controlled mainly through an app on the survivor's phone, but can also be accessed online. They will need a smartphone and stable WiFi within their home to utilize the system. Because of this, it is recommended that general tech safety planning be undertaken to safeguard the survivor's phone, email address and text messages before installing the Ring app.

Smartphone

Because the Ring app relies on the use of a smartphone, it is important to review safety steps around smartphone use. This is especially true if the person using violence is on a shared cell phone plan with the survivor, or has physical access to the survivor's device. Safety steps can include logging into the survivor's cellular provider account, verifying if there is a shared user, updating the password and adding an additional security pin to access the account. There may be state laws that provide avenues to remove the survivor from a shared internet or cell phone account with or without a protective order. We recommend familiarizing yourself with what is possible in your state.

WiFi

As outlined in the Survivor Guide, it is recommended that survivors update their WiFi password prior to installing the Ring device(s). Read the Survivor Guide for tips on how to do this.



Account Password & Set-Up

Ring has already implemented a few security requirements to make it difficult for others to access the account. The Ring account is tied to the survivor's email address and two-step verification is mandatory at login. Passwords must include letters, numbers and symbols (which encourages setting up a unique password) and survivors receive an alert through email and a push notification to your signed-in Ring app if someone logs into their account from a new device.

Suggestions to Enhance Safety

New Email Account

To provide an added level of safety, ask if the survivor would like to create a new email account that no one else knows about to set up their Ring account.

Turn Off Text Message Forwarding

Confirm text message forwarding is turned off on the survivor's device. This process can vary on Android devices and an Internet search based on the make and model of the survivor's device is recommended to determine the proper steps. For iPhones, tap Settings > Messages > Text Message Forwarding.

RING-SPECIFIC SAFETY CONSIDERATIONS

Shared Users

The Shared Users feature of the Ring app allows the survivor to give viewing access to others. Shared Users can view the survivor's live streams and video recordings. If a survivor is concerned about unauthorized access to their Ring device(s), the Shared User settings should be one of the first places to check to see and/or remove a user.

How It Can Happen:

Unauthorized Access: If someone is able to physically access the survivor's smartphone, tablet or computer and open the Ring account, they can add themselves as a Shared User and the survivor would be unaware unless they proactively check the Shared User settings.

Misuse of an Authorized Shared User Account: A survivor may add a household member, such as a child, as a Shared User. This can become a safety risk if someone else, such as a co-parent, has access to that Shared User's account or login credentials. That person could then log into the Shared User's account from their device and the survivor would be unaware.

Before removing an unauthorized shared user, encourage the survivor to screenshot the added account as it may be helpful evidence in the future. Video evidence is discussed in more detail below and in the Survivor Guide.

RING DOORBELL

Authorized Devices

There is a quick way to verify if someone is logging into the survivor's account without consent. The Ring app keeps a log of all the devices that are logged into the account. In the Ring app, visit the 'Control Center' and select 'Authorized Client Devices' to view and confirm they recognize each one and remove any that do not belong. Again, be sure to screenshot any unauthorized devices.

Changing Contact Information: Someone who accesses the survivor's Ring account or app cannot change the survivor's email address, phone number or password without first entering the account password. As outlined in the Survivor Guide, it is still important to reinforce strong device safety practices in survivors with Ring accounts such as maintaining contact with their devices, using updated device passcodes, enabling fingerprint/face ID, etc.

Should They Enable End-To-End Encryption? Security experts recommend end-to-end encryption, which encrypts the video and audio recordings produced by enrolled Ring devices so that they can only be viewed on enrolled mobile devices. Survivors should be aware that they will lose some functionality, such as the ability to add Shared Users, if they choose to activate it.

Video Recordings

Ring devices have an optional subscription plan to save video footage. If the survivor received their device through Ring's donation program, they include the Ring Basic Protect Plan, which allows video footage to be stored for up to 60 days. This time frame can be shortened within the app's Control Center. If a security event does occur, the advocate can remind the survivor they have the option to download and save the footage (as explained in the Survivor Guide).

If an incident is caught on camera, it is up to the survivor to choose if they would like to share the footage with law enforcement or for an ongoing case. Advocates can discuss the risks and benefits of doing so. Local law enforcement may have specific guidelines as to how a survivor can best store footage and work with law enforcement to share footage if they choose to do so.

SAFETY STEPS DURING AN INCIDENT

The Ring device is now part of the survivor's safety plan. While these devices can provide them with a greater sense of safety, it is important to remind them that this does not replace their safety plan. This should be just one piece to discuss as you create a personalized safety plan with the survivor. If a survivor is alerted to an unsafe person at their front door or within view of an external Stick Up Cam, you can plan with the survivor on different actions they may want to take:

Options if the Survivor is Home:

RING DOORBELL

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 they are in the home while fleeing the home.

Options if the Survivor is Not at Home:

1) Ensure that motion alerts are enabled when they are not in the home. The Ring app allows for several customizable settings for motion alerts. For example, a survivor (at home or away) can be alerted whenever a person passes in front of a Video Doorbell or Stick Up Cam. This is helpful to ensure the home is safe before returning home or provide peace of mind while in the home.

2) If a motion alert is received, the survivor can:

- Call law enforcement.
- Speak to the person remotely through the app, acting as they are home or not at home.

WHAT IF A SURVIVOR HAS READ OR HEARD CONCERNING NEWS ABOUT RING?

We believe survivors should be able to make an informed decision about using Ring devices and Ring has received criticism in the past for some of its practices. Some survivors may choose not to participate in a Ring device donation program and it is essential that the survivor understands that participation is optional. Below are some examples of issues that have arisen and how Ring has responded. It is up to your discretion as to how to use this information and how to respond to survivors in these instances.

COMMON CONCERNS

- Third-Party data breaches may make a person's usernames, passwords and other credentials available to bad actors. If a person uses the same credentials for multiple accounts, hackers may be able to use exposed credentials to also access Ring accounts.
- There were previously fewer protections against password hacks. while two-step verification(2SV) was offered by Ring, it was not mandatory
- Law enforcement previously could make direct requests to users for access to their video recordings.

SAFETY MEASURES

- Video End-to End encryption can be enabled to ensure no one has access to your videos. This is an optional setting. By default, Ring already encrypts all videos when in transit and in storage.
- Ring sends alerts by email or push notification for any new login to your account. They also scan the internet and dark web proactively for compromised credentials and alert users.
- 2-step verification is mandatory to log in from a new device, and Ring defaults to SMS as the method for users to receive their one-time verification code . Authenticator apps are also an option to use if a user does not want to authenticate by email or text message. Passwords must be complex and have uppercase, lowercase, numbers and symbols.
- Ring discontinued video requests in 2021. There is now a Requests for Assistance category on the Neighbors feed or app. This is a post category within Neighbors that enables public safety agencies to ask the public for help with an active investigation. Survivors have no obligation to respond to any requests.

SURVIVOR SAFETY PLAN

Technology and Ring Security Devices

The following questions and prompts are steps you may choose to utilize to increase your safety via your technology and Ring security devices. This document is meant to supplement a comprehensive safety plan. You may choose to keep a copy of this document as a record of the safety steps you have outlined, but it is a good idea to keep it in a safe place where your partner is not likely to find it. If your partner becomes aware of this information, it's a good idea to create a new safety plan.

For information on tech safety to assist with your plan, review the Ring Survivor Safety Guide and the Technology Safety Survivor Toolkit (link) by the National Network To End Domestic Violence (NNEDV).

Understanding Your Technology

Safety considerations regarding smartphones include:

- Do you know how to turn off GPS and location tracking on your phone?
- Do you have a shared family plan where your partner could access your account or monitor your calls?
- Is it safer for you to have a separate or prepaid phone?
- Are you interested in separating your line from the family plan?
- Do you know how to check your list of apps to make sure something was not downloaded on your phone without your knowledge?

SURVIVOR SAFETY PLAN

Continued

- Do you have both Face or Fingerprint ID enabled, plus a strong passcode set on your phone?
- Do you know how to check if text message forwarding is turned on? Can you turn it off?
- Other ways to increase safety with your cellphone:

Considerations regarding online safety include:

- Can you create a private email account?
- Is it safe for you to change account passwords that your abuser knows?
- Is there a public computer or a computer of a trusted friend you can use if you're worried about your online activities being monitored?
- Do you know how to delete Internet and search history on your computer and how that can be unsafe in certain situations?

SURVIVOR SAFETY PLAN CONT.

Continued

- If you are trying to keep your location confidential from your partner, try googling your name to see if your location is easily found. Keep in mind to not google your name often.

- Has your abuser ever had access to the WiFi? Have you changed the password to your WiFi?

- Have you named your WiFi something that would not identify it as yours to the abuser?

Other ways to increase safety with your computer and/or online accounts:

Ring Security System Safety Considerations

- Have you set up a strong and unique password?

- Is e-mail/text message safe for two-factor authentication? Would an authenticator app be safer?

- Do you have children or household members that would need Shared User status? Is there a trusted person who does not live with you that you would want to add? What are the risks and benefits to giving someone access to your video feed?

SURVIVOR SAFETY PLAN

Continued

- Do you know how to periodically check and verify the Shared Users and Authorized Devices linked to your Ring account?

Safety Steps When an Incident Occurs

- If you are home, and the security device is triggered by your abuser, what steps might you take?
- Is there a way to leave your house safely?
- Is there a trusted person you can call quickly to contact the police? How would you alert them?
- What is the safest strategy to respond? Would you use the two-way speaker in your Ring device to speak with them?
- If you are not home and the security alarm is triggered, what steps might you take?
- After the incident:
  - Do you want to save the video recording? Do you have a safe place to save it? Would you like to share it with law enforcement or your attorney?