How to protect your phone from SparkKitty photo-stealing malware

Unfortunately, malware is getting smarter and is now targeting sensitive information stored as photos, like the latest SparkKitty malware on phones.

Many people store sensitive information as images, such as passphrases, password manager master passwords , authentication recovery codes, etc. Unfortunately, malware is getting smarter and is now targeting sensitive information stored as images, like the latest SparkKitty malware on phones. This guide lists all the ways to protect yourself from such threats.

What is SparkKitty Malware?

SparkKitty is a variant of the original image-stealing malware, SparkCat. While SparkCat focuses on using OCR to steal specific types of images (code phrases), SparkKitty simply uploads all images to a C2 (Command and Control) server. It is much more dangerous because it is not tied to a specific type of image.

Stolen photos can be used for more than just stealing recovery keys or passwords, such as blackmail, identity theft, and social engineering attacks . It is also difficult to detect because it often comes bundled with phone apps that have legitimate functionality and take advantage of default media permissions. Although common on third-party stores, many infected apps have also been found on official app stores, such as Soex and ?coin (which have since been taken down).

Secure sensitive photos

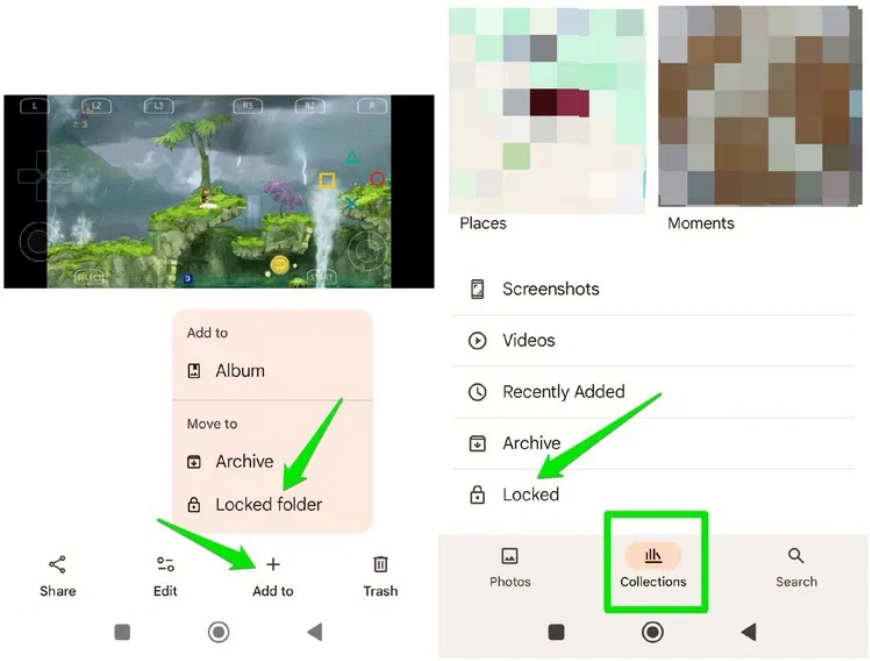
These photo-stealing malwares often target photos inside your library, so your first line of defense is to keep sensitive photos safe. The best way to do this is to hide sensitive photos in an encrypted vault so no one but you can access them. Here are two free solutions:

Using Google Photos Locked Folder

If you sync your photos with Google Photos , you can use the Locked Folder option to store your photos in an encrypted online vault. This will delete the photos from your phone and hide them in Google Photos.

Open the photo in Google Photos, tap the **Add to button at the bottom, and select the Locked Folder** option . You'll need to do a quick initial setup on your first try. To access the contents of your Locked Folder, go to

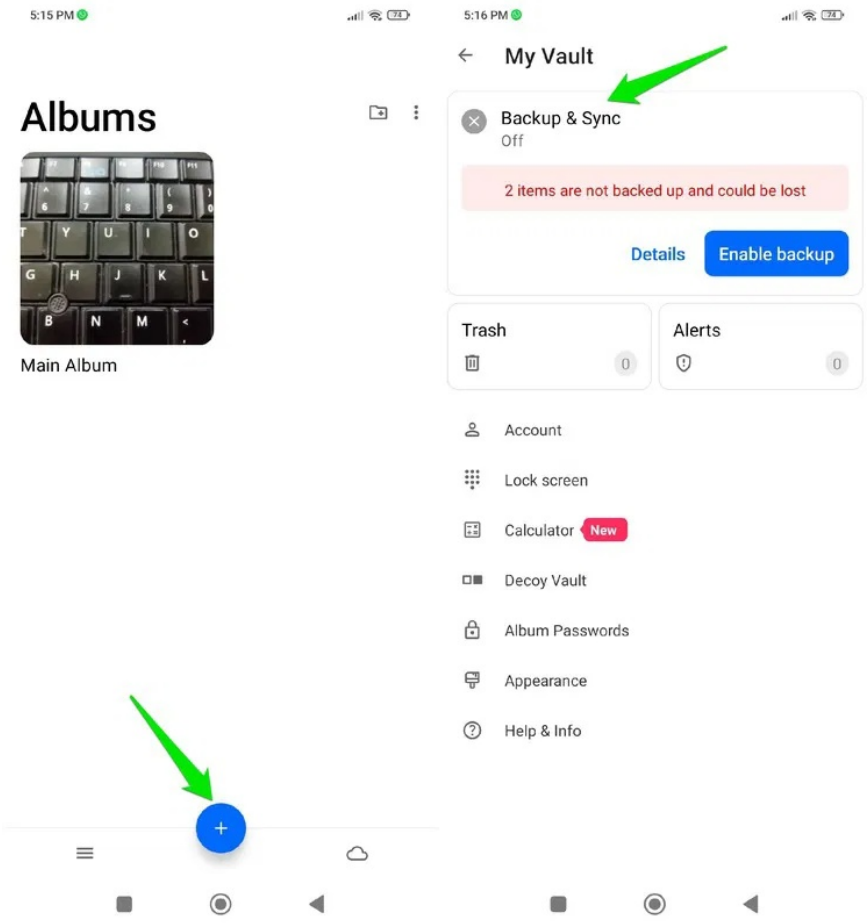
Collections and open **Locked Folder** . You'll need to use a device unlock method to access it.



Using a third-party Photo Vault app

You can also use a third-party photo vault app if you don't want to use Google Photos or want to keep your photos offline. Keepsafe Photo Vault is a great app for this purpose, available for both Android and iOS . The app encrypts your photos (and other media) with a dedicated PIN or biometrics. You can also spoof the app icon to prevent further access attempts.

However, the app syncs photos to the cloud by default, make sure you disable this feature from **Backup & Sync** options if you want offline storage.

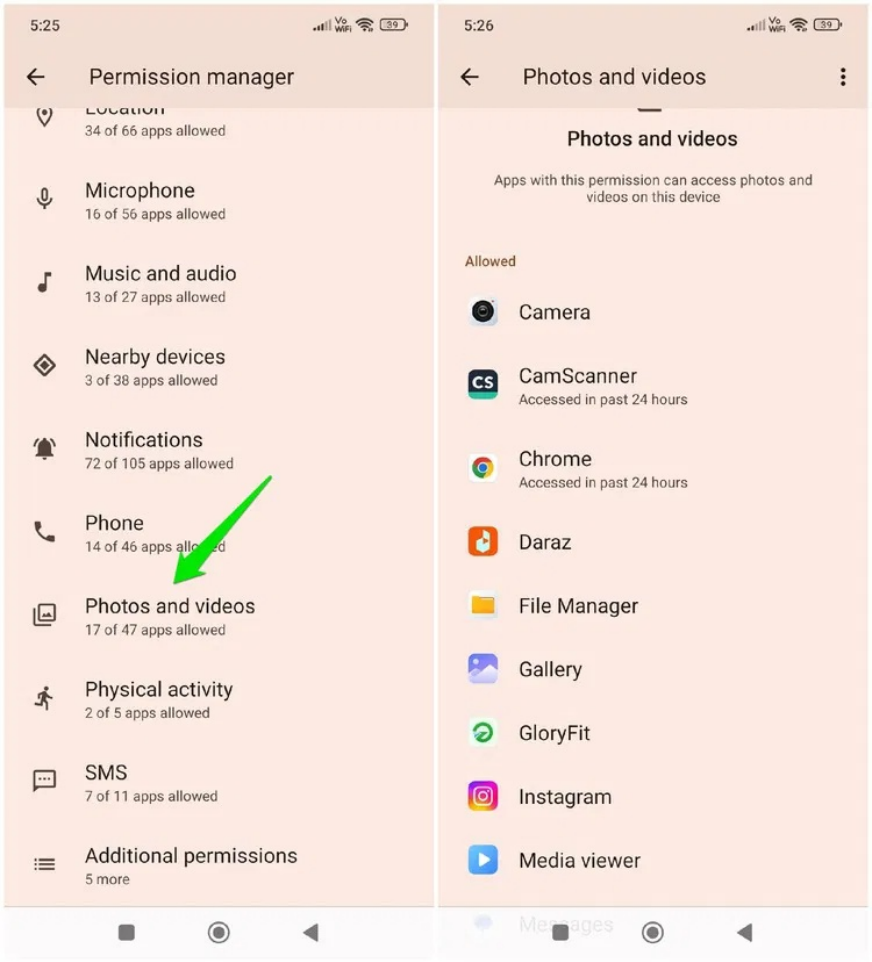


Manage application permissions

SparkKitty needs access to photos to be able to steal them, so the malware app must have this permission as well. You can check the permissions to make sure no unrelated or suspicious apps have access to photos.

1. On Android, go to **Settings** -> **Privacy protection** -> **All permissions** -> **Photos and videos** .
2. On iOS, go to **Settings** -> **Privacy & Security** -> **Photos** .

Here, make sure only trusted apps are allowed to access your photos. If an app looks suspicious or doesn't need media access to function, remove its permissions.



You finished reading the article "**How to protect your phone from SparkKitty photo-stealing malware**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.