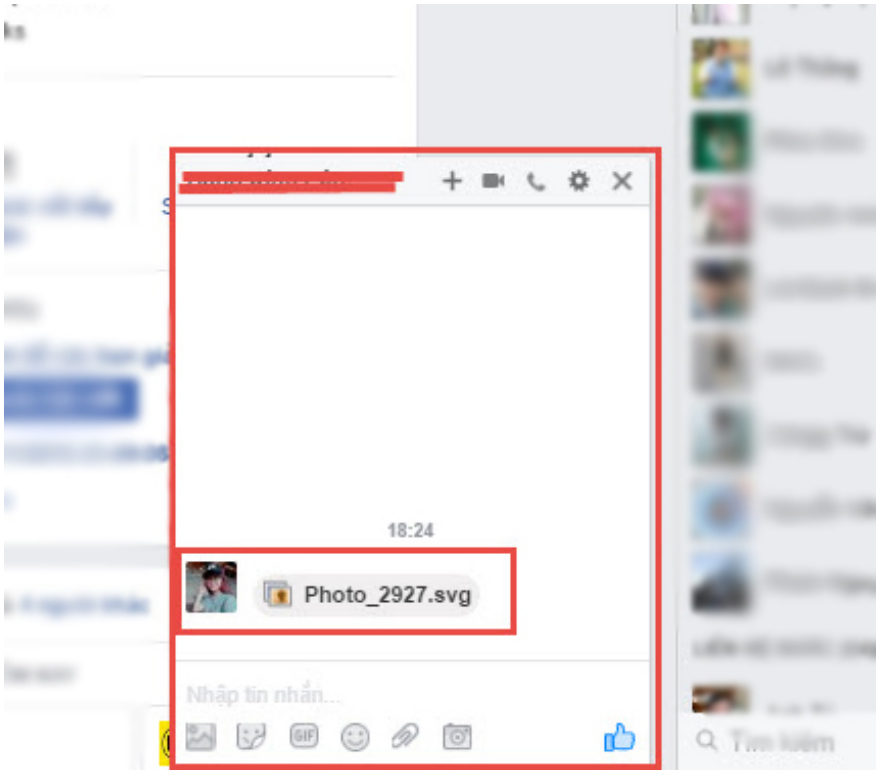
How to prevent .SVG images containing new malware on Facebook

There is a new virus on Facebook now that contains malicious code in the .SVG format. When users accidentally click on, Facebook accounts can be hacked, even spread malicious code to computers and phones.

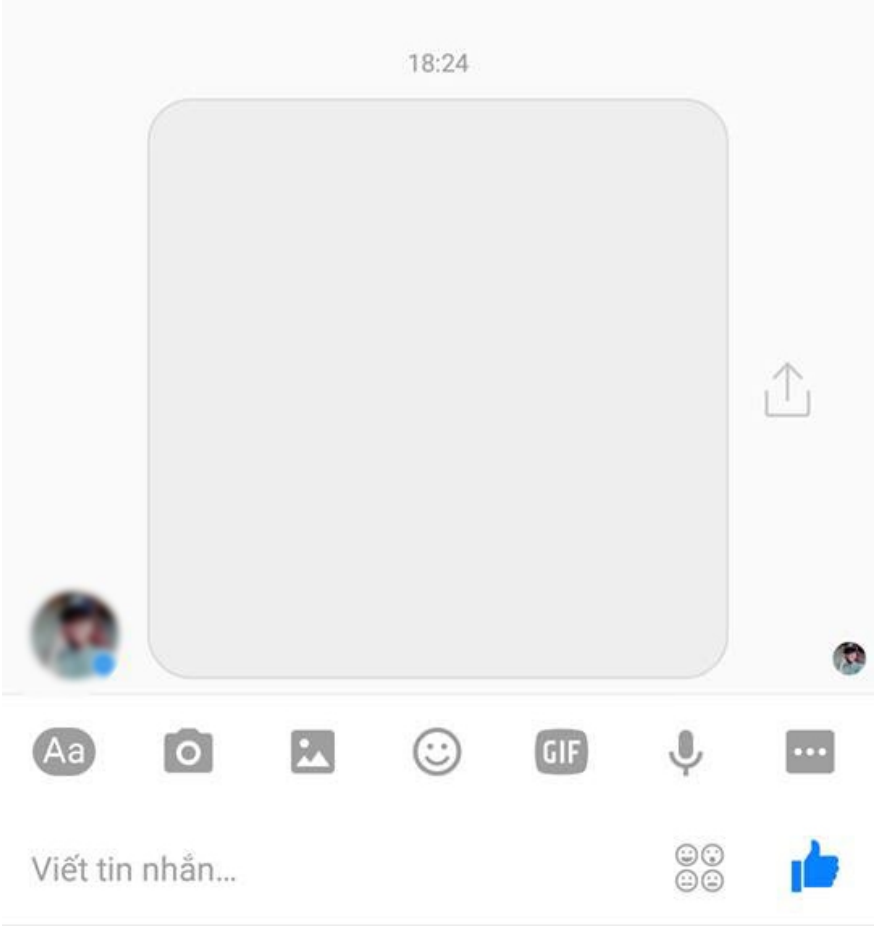
One of the reasons your Facebook account is hacked is the malware (trojan), the virus can even affect your computer or phone. Recently, a new type of malicious code appeared on the Faebook in the form of a white warning image .SVG format, causing loss of account when accidentally clicking or transmitting virus to computers and smartphones. So how does that virus work with how and how to handle it, please read our article below.

1. Facebook malicious code under the image of .SVG:

As mentioned, this new virus form will appear under an extremely normal image, when someone sends you a message. This image will not be completely content and white. But it is actually a form of malware, endangering personal accounts and devices.



The malicious code in the form of the image will be **in .SVG Photo_2xxx.svg format** . If we accidentally click on it will be taken to the grave in some web. The interface will appear bulletin board but there is no content. When you unintentionally press Enter or OK, a series of dangerous utilities will automatically install on the browser, reducing the speed of browsing when accessing websites.



At the same time your Facebook account will automatically send a series of malicious viruses to the friends on the list. And more dangerous is that the Facebook account will be taken away and you can no longer use it. So how to avoid and handle cases that have accidentally clicked on the image.

2. Fix the situation when Facebook attacks malicious code:

When you see a message suspecting malicious code sent to your Facebook with the image format as above, absolutely not allowed to click. Besides, when friends send pictures, the content of the message will appear. If you don't see content, but with the .SVG format, it is definitely dangerous.

1. Change Facebook password:

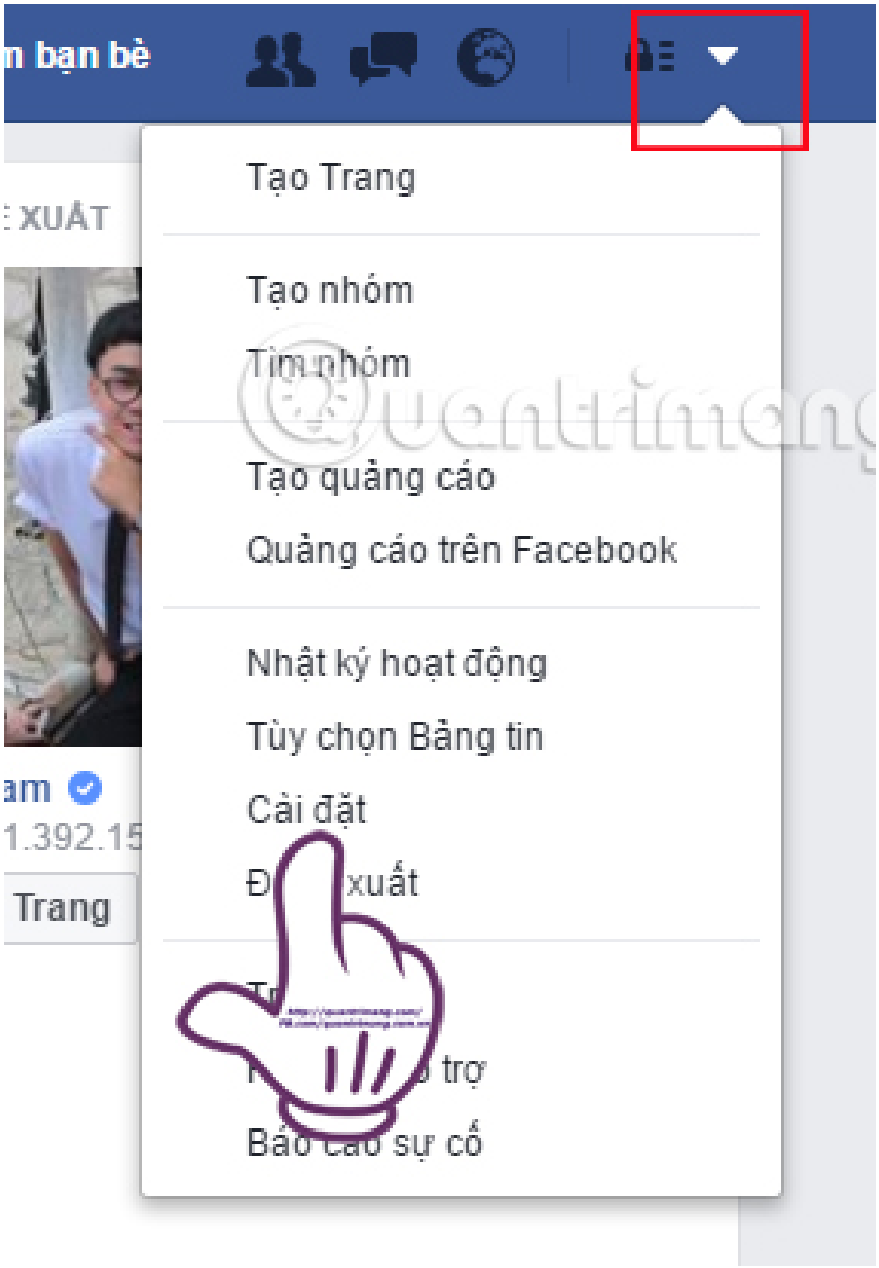
There are a lot of personal Facebook cases that send, spread links to friends, though not by you. As such, your Facebook account must have been attacked by a virus or illegally used by someone. The best way is to **change the new password** , with special characters, uppercase and lowercase letters, which may include numbers to increase security.

2. Check the entire Facebook application:

Facebook now also incorporates many applications for users to search, bringing more fun when using Facebook. However, if there is no need to use those applications, it is best to remove them, to avoid those types of applications that contain viruses.

Step 1:

At the main interface on Facebook, we click on **the drop-down arrow to** the right of the interface and select **Settings** .



Step 2:

Next, click on the **Applications** button in the menu column on the left side of the interface. In the **Log in list with Facebook** will be the applications we have used. Click on **the X to delete applications that** do not need to be used. Or if you suspect any harmful application, you should delete it immediately.

Step 3:

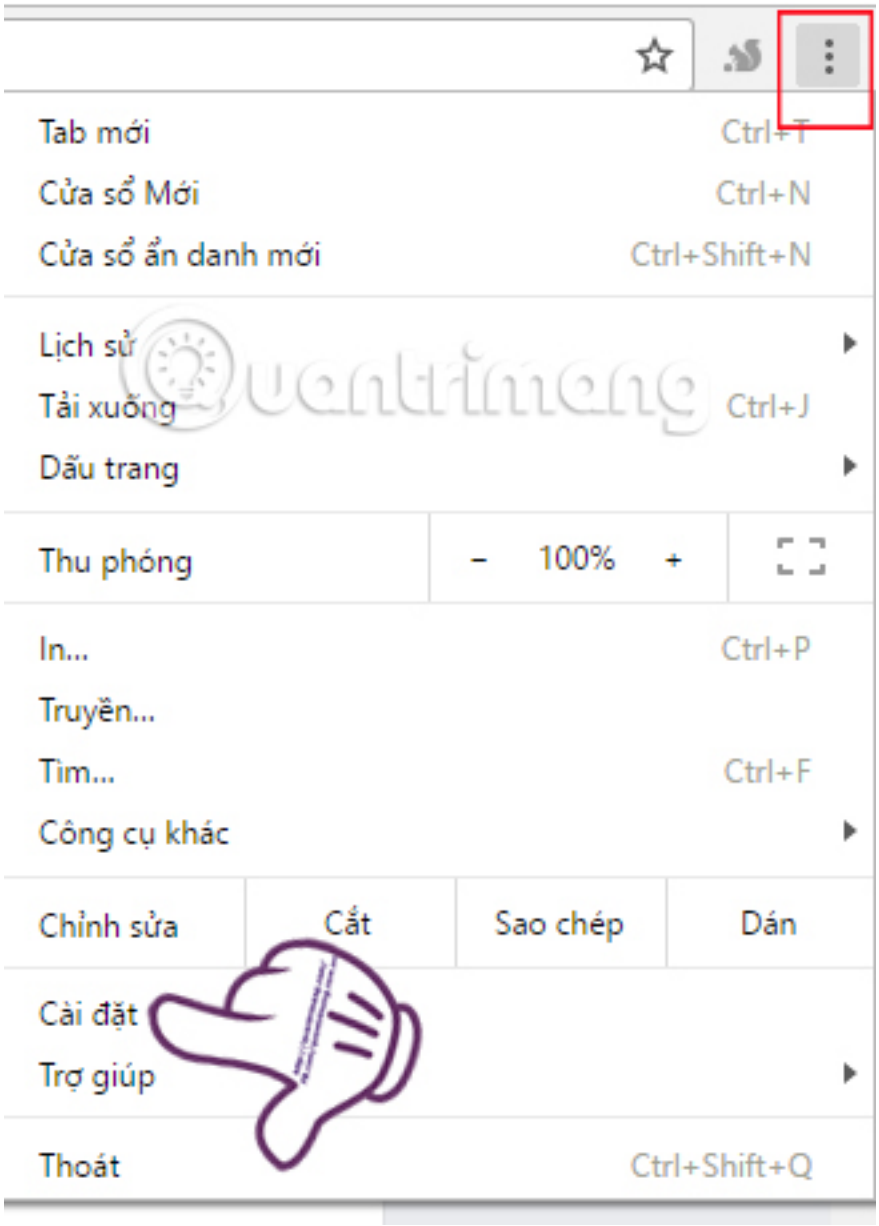
Next comes the application uninstaller interface. We check the box **Delete all activities of the app on Facebook, including images and related videos** , then click **Delete** .

3. Remove add-ons on the browser:

When we accidentally click on the image containing the malicious code, the junk utility will automatically be installed on the browser. So, quickly delete all those utilities. In this article we implemented with Chrome browser.

Step 1:

At the browser interface, click on **the 3 dot icon** and select **Settings** .



Step 2:

In the **Utilities** section, please **delete all the strange utilities** that are not installed by you from your computer. Click **the trash icon** to delete the utility in the browser.

Facebook is now a place to easily spread dangerous viruses, malicious code and anyone's Facebook account can become victims. To limit this situation, it's best not to click on strange links. In case of receiving malicious images like above, do not click on the image but please leave a message to your friends to make sure that they really sent you. And finally don't forget to use secure 2-layer security methods for your personal Facebook account.

Refer to the following articles:

1. Clean Virus on Facebook in just 9 simple steps
1. How 2-layer security for Facebook?
1. How to secure your Facebook account so it won't be hacked?

I wish you all success!

You finished reading the article "**How to prevent .SVG images containing new malware on Facebook**" 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.

© 2019 TipsMake.com