How to prevent malicious blackmail JPG code via Facebook Messenger

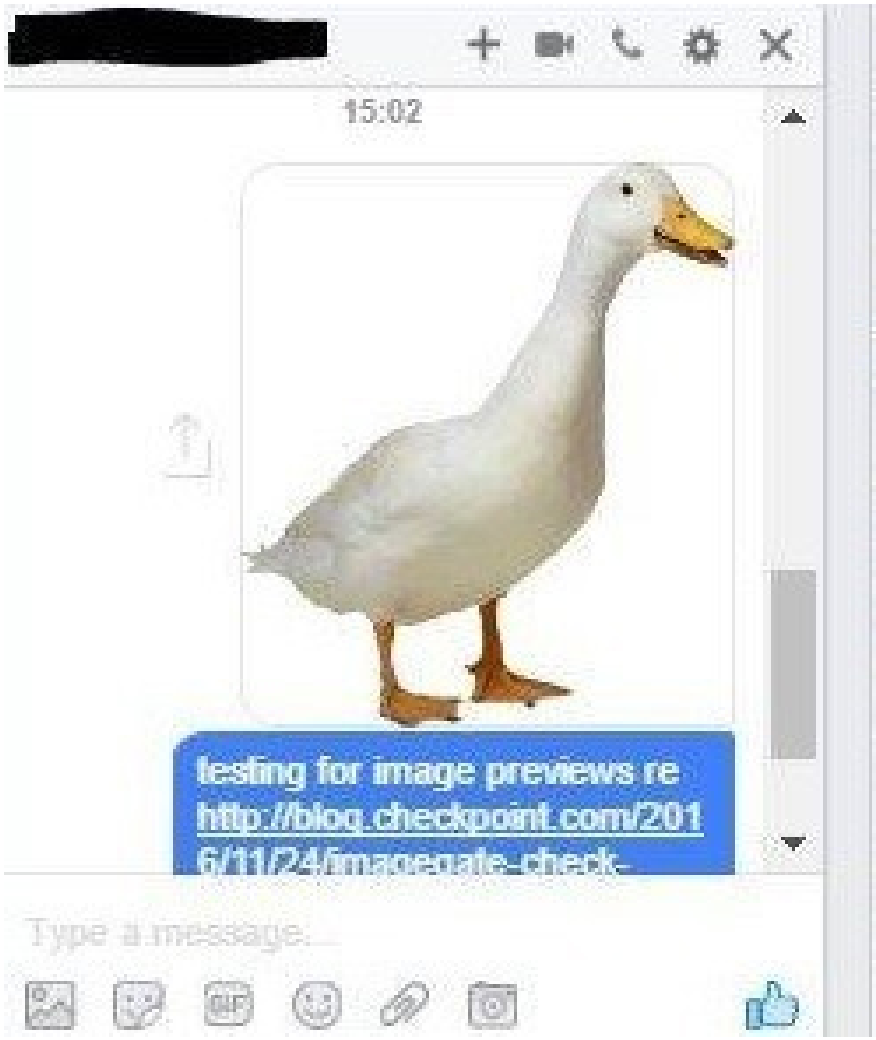
Locky Ransomware is a blackmail malicious code in JPG format on Facebook. This type of malicious code will restrict access to or use of some folders and files. If accidentally infected with this type, Facebook users will be required to use the money to retrieve the account and data

When Facebook users are being warned by a SVG image virus, another extortion code is also attacking your Facbook account in JPG format.

If the user accidentally clicks on this malicious image link, the malware Locky Ransomware will automatically propagate to your computer, disallowing the use of some folders, files or restricting access right away. on the device. Besides, we will get a request to redeem Facebook personal accounts and data with some money. So how does this malicious code work? How to prevent this malicious code? Please refer to the following article of Network Administration

1. Locky Ransomware malicious code via Facebook JPG image

Like the SVG **malicious code** , this **Locky Ransomware extortion code** will hide under the usual JPG format images, and be sent via Messenger messages on Facebook.



The virus was named **ImageGate** by Check Point Software Technologies. When you receive a JPG-form picture message with a malicious code attached and clicked, the malicious code will be spread on Facebook and then on the computer, even download additional .hta files. Since then paving the way for the Locky Ransomware malware to infiltrate the device we are using, requires a ransom to retrieve important data, but has not confirmed that the data is actually returned. with you or not. So how to prevent this kind of malicious code?

2. How to prevent Locky Ransomware Facebook Messenger

1. Don't click on the strange link on Facebook:

Whatever kind of malicious code is transmitted in the format of a link on Facebook, the first Facebook account protection method is to not click on any strange links. With malicious code under JPG format, it is more difficult, because this is an extremely normal and characteristic format. So if you get this JPG image link from a friend or anyone, it's best to contact that person to see if they sent the file to you.

2. Using Facebook security methods:

One of the reasons that your Facebook is easily attacked is because the account security is not tight. First of all, please change the password for your Facebook account, using special characters such as lowercase letters, uppercase letters, numbers or other special characters.

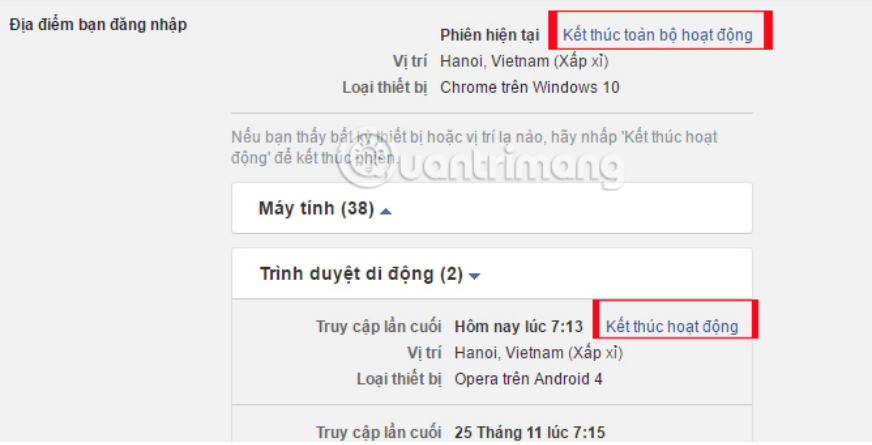
1. Instructions for changing Facebok passwords on computers
2. How to change the Facebook application password on your phone

Besides, we should use 2-layer security method for Facebook account. When we use the phone number and receive the security code for our Facebook account, a security layer is built when requesting a security code if anyone illegally signs into your account.

1. How 2-layer security for Facebook?

Or if you are notified that someone is using your Facebook illegally, we can perform remote logout of your Facebook account.

1. Instructions to log out of Facebook remotely when hacked account



Above are some methods to help us secure our Facebook account, to avoid the ImageGate virus, to pass Locky Ransomware extortion code on Facebook. In any case, you are not allowed to click on any suspicious links. And building security methods for Facebook before being hacked is essential.

The transmission of ImageGate virus extortion code on Facebook

Refer to the following articles:

1. How to permanently delete Facebook account
1. How to recover deleted messages on Facebook
1. Instructions for setting up Live Stream feature Facebook videos on mobile and tablet

Hope few posts above useful to you!

You finished reading the article "**How to prevent malicious blackmail JPG code via Facebook Messenger**" 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