Protecting Yourself from Facebook Scams Have you ever been spammed by facebook messages? Do you know someone who has? Did you know you could be spammed by facebook messages much lilke email messages? Well if it has happened to you then you know what I am talking about and if you were not aware, yes you can be spammed by facebook messages.
 With over 800 million active users (as reported by facebook), the number of potential victims grows rapidly as more and more new facebook profiles are created. With such a huge subscriber base, it really is no suprise that facebook is targetted as a playground for phishing scams, malicious spam and malware. Spam is unavoidable if you work and/or play online. It is not only a nuisance but also a potential threat to your privacy and computer security. Fake advertisements and phishing scams make their rounds through Facebook and other social networking sites just like they do with our emails.
 The most common type of Facebook spam is a wall post that encourages you to install a Facebook application. The application will require you to agree and allow the application to post on your wall and your friend's Facebook wall. Once you allow this authorization, the spam message is immediately sent to your friend's walls. When a friend sees the message and performs the action, he or she will then see the same spam on their wall and the cycle continues. This is how spam messages quickly spread through Facebook.
 How do you protect your Facebook account? If you do not immediately recognize these bogus inbox and wall posts you could inadvertently open your account, your computer and your friends to the scam &#65533; without even knowing you are doing it. Like email spam, one way to stop Facebook spam from spreading is to learn about it, malware and phishing messages. Know how to spot them and also familiarize yourself with how these Facebook spam messages work.
 Facebook does have a number of security controls in place and the system is able to detect many of these types of messages before they become rampant on Facebook. In some instances you may be asked to verify a "Like" or you may see a warning that a link you are trying to visit has been classified as potentially abusive by Facebook.
 Being aware is the only way you can prevent these messages from spreading. Know what to look for to determine if a wall post or inbox message is a legitimate message from a friend or spam. The following tips will help you diffrentiate between spam and legitimate messages.
 <ul style="text-align: justify;"> Look at the message.Is it of the same value as other messages this friend would typically post? For example, if your friend is a professional acquaintance and you see a message like "OMG! Look at this video" on your Wall,

chances are the message was not intentionally sent by your friend. If the message seems out of character for your friend who posted it, then do not click the link. Look in your Facebook news feed.Are you suddenly seeing this message appear multiple times? If so, chances are it is a scam that is being sent through automated means. Pay attention to the authorization requests for any apps you install.For example, to view a video a Facebook app shouldn't need to access all of your information or need permission to post to your Wall and your friend's wall. Always investigate those apps that ask permission to post on your Facebook Wall and your friend's Wall. Be wary when a message on your Wall contains short links from friends who don't usually post links on your Wall. This also is another form of the message being "out of character" for your Facebook friend. Always verify URLs before clicking. In video spam messages, for example, the message indicates you will go to YouTube to watch the video. If you move the mouse cursor over the link (but do not click it) look at the details of the link in the footer of your browser. This will show you a URL that may look similar to YouTube but is not the real YoueTube.com web address. If you click the link and are greeted by an unfamiliar screen and a page you were not expecting, do not click any links or icons on that page. The golden rule: If the message looks suspicious delete it from your Facebook wall. As you move your mouse cursor to the top right area of the Wall post an X will appear. Highlight the X and you will see an option to Remove the post.   How to Remove a Malicious Facebook App? First, make sure you have deleted the post of your Wall to prevent others from seeing the message. The next step is to remove the application from your Facebook account and revoke the access and authorization privileges you granted when adding the app.
 From the top right-hand corner of your Facebook profile: Click Account and select Privacy Settings. The bottom left-corner of the Privacy Settings Page will have a link to Apps and Websites. Choose the Edit your settings link. In the next screen you will see a list of the most recently accessed apps in your Facebook account. Select the malicious spam application from the list, Edit Settings and click Remove.