Link Protect

Protect Links and Images from Unauthorized Linking

For the protection of links to images, other web pages and other linked media. Link Protect can prevent unauthorized linking to images and other media found on your web pages, including links to other web pages and embedded media, protecting them and their content from site grabbers, unauthorized linking activity and bandwidth theft.

Before you can use Link Protect, you must have a cgi-bin in your web site. Check that you do have one and that you have permission to use it. Link Protect will run on both Unix and NT web servers.

- Prevent unauthorized access to your web images and content.
- Check that the call for your image(s) is from an authorized site.
- Eliminate bandwidth abuse completely.

About Link Protect

Link Protect is designed to stop external links to your files, either from other websites or direct entry of a URL. The links calling your pages and images are delivered by Link Protect, which checks the referring URL. Any type of file can be protected with Link Protect - gif, jpg, html, exe. The files are stored in a location inaccessible from a direct URL, so there is no way in the world (wide web) to link to your files other than through Link Protect.

Link Protect is not designed to prohibit access to your files - it simply controls access to your files from external links. Users will still be able to view your website normally, but now you have control over what and where it is downloaded. You can specify domains from which you will accept links such as your other sites or those of authorized associates. Any attempt to link from somewhere else will result in an error message (in the form of a nice big image saying "Invalid Domain"). Your protected content is stored in a folder only known to Link Protect. When a link is clicked or a call made for the page through Link Protect, the software will check that the call is from an authorized site. If the referring address is not listed as an authorized site, a default image is displayed instead of the content.

Unauthorized linking

Link protect checks the location of the caller against your list of approved links. Each call for an image or page is controlled by Link Protect which verifies the origin of the call. If the request is not from within your web site or from one of the authorized, a customized error message is delivered instead.

The image on the server remains completely safe until it is legally downloaded, from your authorized links. Pages and images linked with Link Protect do not reveal direct links to search engines and site grabbing software so that your pages are safe from harvesting.

Licensing

A self-install license is available for per site. If you would like ArtistScope to install Link Protect on your web site for you the installation fee will cost the equivalent of one extra licence. Before you can use Link Protect, you must have a cgi-bin in your web site. Check that you do have one and that you have permission to use it. Link Protect will run on both Unix and Windows web servers.

For Windows and Unix web servers

NOTE - To install Link Protect you must have a CGI-BIN.

Once installed all you have to do is begin addressing your images and pages via Link Protect. You can use any editor to address your images and then later paste the prefix into the address lines.

Link Authorization

With no permissions set the default is that all links being served must be from your web site. To allow linking to your content from other web sites, you can add and delete the site URLs in the script.

Custom Error Message

Bad-domain.gif is the image people will see if they try to access your files from an invalid domain. You can change this image to anything you want - the image provided is a plain and boring message, but feel free to have some fun with it.

Bad-file.gif is the image people will see if you make a boo-boo and create a link to a file that doesn't exist. Once again, you can go for your life with customizing this image.

INSTALLATION

- After unzipping, make a back copy so the original files can be recovered configuration if needed.
- Add acceptable domains to the domains.dat file using Notepad, one url per line with a hard return.
- Upload the folder called "securefolder" to your web site. It is better to rename this folder, but you will have to make the change in the first lines of the cgi also. This folder and all files in this folder need to be writable. The dat files in the "admin' folder should be CHMOD 666.
- Edit the first few lines of each cgi and upload them to your cgi-bin using ASCII. Then CHMOD them 755. Note the difference between paths and urls - do not vary this. If a path is noted in the example, always use the path. If a url is used, then you can use the http:// links
- Once you have seen it working with your new configuration, then it is advisable to change the admin password with Notepad.

Using Link Protect

Once you have installed Link Protect files on your web server, you are ready to start using it. All you need to do is place your protected files in the Secure Folder and change the links on your pages to point to Link Protect.

The standard way of calling a protected document is as follows:

Click Here!

where filename.html is the file you want to display (which can be any type of file). You may have to adjust the reference to the cgi-bin to match your system - you may even need to use an absolute reference to a different domain.

If the protected file is meant to be downloaded rather than viewed in the browser, you will want to supply the browser with a suggested filename for users to save the file under (if you do not do this, protect.pl will be the filename - even if they are downloading a zip file). This is done by sending extended information to the browser:

Click Here!

If you look carefully you will notice "/download.zip" after protect.pl and before the ? This is the filename that the browser will prompt the user to save the file with.

Link Protect can also be used to display an image on the page:

<img src=/cgi-bin/protect.pl?File=my-image.gif>

In this case, the file will have to be either a jpg or a gif so that the browser can display it. Other tags within the <img> can also be used, such as alt, border, etc.

Secure Folder

Only Link Protect knows the location of your Secure Folder. It can be set to any folder on your site and contain sub folders and so on. The Secure Folder is the root of the directories in which your files can be placed - you can create subdirectories of it to give you some ordered structure. When you do this you simply need to include the subdirectory after the File= i.e.:

Click !

The system is secure is long as no direct links are made from any pages on site. It is the direct hyperlinks that spiders use to trace the location. Also, the visitor can no longer find the direct route to the content by following the source code.

The default setting for the protected folder is "securefolder"... this should be changed and also altered in the CGIs otherwise other users will know where the folder is.

Error images

The image that is displayed when an error is made or someone uses an illegal link can be customized to anything your want to use. If you make a new image, simply rename it to replace the ones on the protected folder. If you don't change its location or name, you won't have to modify the cgi.

Known Quirks

The two inserts below are space sensitive. Should you edit the files that contain these inserts in a html editor they could be corrupted by adding space around the inserts. There should be no spaces before and after each insert and they should be hard left to the margin as seen below...

<!INPUT VARIABLES>
<!INPUT DOMAINS>

Access denied

On some servers and services when the CGI is first installed and tested even though the scripting and codes can be correctly set, the Access Denied image is delivered. This can happen at first even though everything is correct. We are not sure why it does happen and can only guess that it has something to do with FrontPage or proxy servers updating links. Whenever we have returned the next day everything has then been seen to be working perfectly.

Image Distortion

When linking an image through the CGI from a page already served by the CGI some editors will set the image size to the bad-domain.gif, to overcome this you may have to remove any reference to the image size in html and allow the image to be presented as is... at its original size.