CopySafe Web Insert

The “Insert” version of CopySafe Web does not involve the use of the image encryption software normally supplied with the full version of CopySafe Web. Instead, a pre-made image applet is provided with examples of code to add to existing pages on your web site that you want to protect.

To enable copy protection via the interaction of the CopySafe plugin, all that is required is the small security applet (as supplied) which you can place anywhere on your web page.

From the example found on the “CopySafe page” folder you can see the parts needed to use. The main parts are the applet itself and the csi_insert.js insert tags just below the applet.

CopySafe page sample

The sample CopySafe page shows an example of the code required for maximum protection. Note that included in the page is a Java version checking applet that checks to ensure that the visitor has the minimum Java version required which is Java 1.4.

This page is given as an example only and it won’t be necessary to include the Java version applet if you use it on any pre-entry pages that contain an index to your copy protected pages. In fact the recommended methods is to not use it on the CopySafe page as it is trigger sensitive in that if you have any script errors on the page at all, it will trigger a redirect for Java download. That is how the version checking works.

Java version check

The Java version check is very sensitive to errors and it is the only way to check Java version in all browsers. To remove Java version check, first remove the “onLoad” statement from the <body> tag and then remove the JavaScript routine from the head tag.

Csi_insert.js insert file

Using different insert files will enable you to vary the security level between folders. Each CopySafe Web page can be set to allow/disallow capture, keyboard and menu options:

- CaptureSafe = 1 or 0 for allow screen capture
- KeySafe = 1 or 0 for allow use of the keyboard in web forms
- MenuSafe = 1 or 0 for allow browser menus
- RemoteSafe =1 or 0 to allow remote viewing of the page

The csi_insert.js file contains the triggers for CopySafe Web and manages updates to the latest version if a visitor doesn’t have a plug-in or has one of an earlier version.

The csi_insert.js file can be used in the same folder as your CopySafe Web pages (one in each folder) or you can use the one csi_insert.js file to serve all CopySafe Web pages by placing it in the root of your web site and adding a backslash as follows:

```
<SCRIPT SRC="/csi_insert.js"></SCRIPT>
```

Adding a backslash tells your server to look in the lowest level of your web site when you want to use the same js file for all pages. For example: /csi_insert.js. Or you can use individual js files for different folders that can set to allow/disallow some features such as print, menu/keyboard and capture (see further below).

Control of allow/disallow print/keyboard/capture

Caution: Disabling any security function not only opens doors to your content, but it also allows visitors to get an insight into how the CopySafe Web system works, which up until now has been most obscure. The only option we do recommend is for allowing the use of the keyboard and only when necessary such as in the case of online surveys and order forms.

Although not recommended in situations where absolute security is required, you now have the option of reducing the level of security applied to your whole site or to individual folders. This can be useful when used in conjunction with order forms that require the use of the keyboard or when you want to allow visitors to print a page but not use Printscreen or capture.

The EMBED tag

On any new pages made by the program you will see an EMBED tag. This tag is required for Netscape browsers and should always load last. That is, after the main body of text, images and code on your page that is found within the BODY tags. Failure to ensure that the EMBED tag loads last will cause errors and plugin detection to fail in Netscape browsers. Below is an example of the tag with all options set for control (as found in the default template file).

Each parameter has a value of 1 for on or 0 for off. By default they are all on so leaving out the options gives default CopySafe Web behaviour.

- CaptureSafe - detects and kills screen capture apps, jumps browser to the non-compliance page where necessary.
- KeySafe - locks the keyboard, prevents system keys like alt-esc and print screen. Turning this off allows the user to fill in and submit forms.
- MenuSafe - prevents access to menus. Turning this off will enable printing.
- RemoteSafe - prevents access by users using remote or virtual computers.

The body tag script

The script routines within the body tag add extra security by preventing such things as drag’n’drop whereby a visitor may otherwise be able to select an image on the page and drag it to the desktop.

Protecting non-image files

Although CopySafe Web was designed to protect images by encrypting them and displaying them in our security applet, with careful coding CopySafe Web Insert can be used to protect almost all content that can be displayed on a web page.

Protecting normal pages within a frameset

A frameset is a page arrangement that enables several pages to be displayed in the same browser window. By using a small CopySafe Web applet within the static page (such as the header or menu page for the frameset) you can protect all other normal pages opening in that frameset. To use frameset protection please observe the following:

- Firstly, disabling any of the security functions with the csi options is NOT recommended with frameset use at all.
- Each page belonging to the frameset needs to be protected from opening outside the frameset by using a JavaScript. Add the insert tag to your page header tags and then add the following line to the body tag where the page link is that of the frameset itself: onLoad="tmt_backtoframe('index.html')”
- All links given from the frameset pages must be targeted to the respective frame names.
- All links given for pages outside the frameset must use target=_top.

Protecting from direct linking

Allowing visitors to bookmark your protected pages and return by using a direct link (and not from a link within your web site) is not recommended. There are many ways to ensure that this doesn’t happen depending on the script format supported by your web site. For example if using FrontPage, which supports ASP, you could use the following code:

```
Dim strCheckReferrer
strCheckReferrer = Request.ServerVariables("HTTP_REFERER")
If strCheckReferrer <> "" then
        Respose.write"<your html goes here>"
        Else
        Response.redirect"/protected_index.asp"
End if
```

Here the ASP is checking for a referrer. If they are using a bookmark there will be no referrer and they will be redirected to your index page.

If you want to further protect to ensure that they are not following a link from a forum or another page outside of your web site you could use the following code:

```
Dim strCheckReferrer
strCheckReferrer = Request.ServerVariables("HTTP_REFERER")
If strCheckReferrer <> "" then
   dim AA, BB
   AA = Lcase(strCheckReferrer)
   BB = "mysite.com"
   if InStr(1,AA,BB,0)>0 then
      Response.Write""
   else
      Response.redirect"/protected_index.asp"
   end if
end if
```

Here the script is checking that the referrer is your web site ensuring that they have accessed the protected page from a link from within your web site. For this to work properly the referrer has already been converted to lower case, so what you write in as your site for BB should be lower case also.

Note that the FrontPage web page must be named as an ASP page, for example "exhibit_1.asp"

Customizing the security applet

The image supplied is fixed and cannot be changed. To use a different image you will need the full version of CopySafe Web. However you can customise the look of the applet. For example you can change the background colour of the applet to suit your page colour, and you can add a link to the hyperlink parameter so that visitors can click the padlock icon to escape CopySafe control. Here you can set a link back to your protected index or to your home page. Of course you will need to add a statement to you page such as "To escape CopySafe controls, simply click the padlock icon".

Plugin downloads

To provide plugin downloads for your visitors, simply copy the "plugins*" folder to the root of your web site and ensure that the URLs listed in the top of the csi_insert.js file do match.