

Be careful... hidden eyes are snooping at your document.

There are times when business organizations have to permit sensitive information to be seen by others. Generally these documents should be accessible only within the internal network, but one has to permit key people like fund managers and major shareholders to access the same. Most organizations keep these pages, where the sensitive data is accessible through an external network, under a password protected index page.

However, it is common knowledge that any hacker worth his salt will be able to bypass the password-protected page within a few hours. This leaves the sensitive data of the company in peril since all and sundry can view it, especially if the hacker copies the page and hosts it on any unprotected server. This can be dangerous, especially if rivals can access the data.

Your plan of reducing the price of a few products during the festival season is now known to your rivals and you can be rest assured that they will surprise you with even lower priced products on the same day that your organization is planning to reduce its own prices. In the past if such a breach had occurred, nobody could be held liable, but these days have gone.

Board managements know that they have to keep secure information secured. If they do not take care to see that it is secured, the breach of security might well lead them being prosecuted. There are many suppliers who promise to keep your files secure, irrespective of the file type, which can be .html, .pdf, .jpg or .gif. For their services they charge a hefty sum of money.

Why pay them that extra amount when you can do it by yourself with the use of dedicated software? There is no steep learning curve and anyone with a slight knowledge of computers can use the same. The state of the art DRM software controls ensures that all your sensitive data are protected with copy protection routines. Apart from prohibiting others from editing or saving vital data, these specialized software pushes up the safety routine a notch higher.

The moment a protected file is opened, the software disables the print screen key. If you do want someone to access and print a copy of the file, you can add watermark images to the output so that they cannot be reproduced further. Adding a fine screen on the background will make it tough to copy the printed document. While pirates of sensitive data are always trying novel approaches, you have the option to be one up on them.

About the Author

Have you given a thought about ensuring [regulatory compliance](#) in your organization? [Document retention](#) time can be reduced with [copy protection software](#).

Source: <http://www.zero-zero.info>