NAME	Dolphin Secure
Company	Dolphin Media Germany AG
Version	1.0.13
Type of product	Client
Devices supported	Computer
Operating systems	Windows XP SP3 (32/64 bit) Windows Vista (32/64 bit) Windows 7 (32/64 bit) Mac OS X Version 10.5 or later version (32/64 bit)
Price*	1 license: 19,95 €
Language of interface	German
GLOBAL RANKING	**As effectiveness was not tested on this tool, no global ranking could be calculated.**

*Prices might change according to the latest company offers

User's voice

Comprehensibility:

Look and Feel:

Time to install and configure:

52 minutes

2 test user

"I missed the detailed information about the usage (of the product) for parents and children (...)."

Test user placed in: Germany

Test user´s degree of internet literacy:

0 100

NOTICE

Dolphin Secure significantly differs from tools tested under SIP-BENCH II project. Basically, the tools act as filter, i.e. they block or allow pages which users want to open. The criteria for blocking/allowing the page are usually as follows:

- A list of pages labeled as harmful (black list).
- A list of pages labeled as non-harmful (white list).
- Analysis of the page requested by the user.

The filtering process is performed on all the Internet pages.

Dolphin Secure is not a filtering tool but a closed *kindergarten* or walled garden. It gives access only to selected websites ranked as suitable for children.

- ✓ Advantages: this approach ensures that a child will not see any harmful content.
- ✓ Disadvantages: a very small part of the Internet is accessible.

This approach can be suitable for children but not for teenagers. It should be noted that other tested tools can be used, with a specific configuration, as a walled garden, allowing a child to navigate only through a list of websites chosen by the software producer or the parent (white list only navigation mode).

Special notice for appropriate usage
In Dolphin Secure the black list and the white list operate together but the white list takes precedence over the black list. This means that when a user begins using Dolphin Secure, he/she can access only 700 websites available on the white list so far. With the Admin password, user can overrule the white list and add additional sites on the white list. Therefore, the Admin can switch sites from the Dolphin black list to the white list, except for those that are listed on the additional German blacklist called BPJM-Modul. BPJM is an official German index of websites marked as harmful for kids and teenagers.

FUNCTIONALITY

This tool responds to a different conception of filtering tools than those generally included in this benchmarking study.
The tool allows websurfing through a specific interface provided by the filtering software company. The tool works with a white list (German only) and the parent can only decide to add new websites to the white list or to blacklist some specific website included in the whitelist. The idea is that of having a sort of closed safe *kindergarten.* Also external contacts are possible only among those already registered to the community and authorized by the parents (not included in this testing activity). Each license allows one child-user only.

FUNCTIONALITY SCORE: 1,0 OUT OF 4 POINTS

EFFECTIVENESS

As the tool operates as a closed *kindergarten*, effectiveness could not be tested. Indeed no harmful content is displayed to the user and almost all non-harmful content is blocked.

USABILITY

Installation of the tool: The installation process is short and well comprehensible. The installer does not provide advanced options and cannot be influenced with regard to kind or amount of information, except for the language. The process is consistent and it is conform to users' expectations.

Configuration of the tool: The configuration process is mostly well comprehensible, but it is not overall easy to learn. Information is missing with regard to format and values of configuration parameters. Also error messages could be improved. The process is mostly consistent, but it is not overall conform to users' expectations. The design is appealing and joyful.

Usage of the tool: The user has the option to sign on with a fingerprint scanner thus no password management is required. This is generally comfortable, but might not be easy to operate for all users. The tool provides the option for the child to contact the parents directly via email, when a web site is blocked. The alert message cannot be customised, but it is adequate and child friendly. The tool offers no reporting.

Usability of the installation process: 2,81

Usability of the configuration process: 1,84

Usability of the usage of the product: 2,73

OVERALL SCORE FOR USABILITY: 2,30 OUT OF 4 POINTS

SECURITY

IMPORTANT: the tool filtering action failed with the inclusion of "google.de" in the whitelist. The tool let the user access also porn websites through the google search.

OVERALL SCORE FOR SECURITY: 2 OUT OF 4 POINTS

DETAILED FUNCTIONALITY FICHE

AREA OF NEED	FUNCTIONALITY	SPECIFIC ISSUE	ASSESSMENT
MGMNT	**Management of users profile**	Create several profiles	NO
	Monitoring	Remote access	YES
FILTERING CUSTOMIZATION	**Topics**	Customisation of filtering topics	NO
	Urls White lists	Restrict browsing to a white list	YES
		Default white list	YES
		Modification OR Creation	Modification – YES
			Creation – NO
	Urls Black lists	Creation of user's own black list	YES
KEYWORDS	**Keywords**	Default black list	NO
		Default white list	NO
		Creation of a user's black list	NO
		Creation of a user's white list	NO
TIME	**Time limit settings**	Set a specific timeframe or web access duration	NO
BLOCKING MESSAGE	**Type**	Ask for unblocking to parents	YES
		Redirect to safe resources	NO
USAGE RESTRICTION	**Web**	**Block** access	NO
		Monitor access	YES
	Safe Search	**Availability**	NO
	Social Networks	**Block access**	NO
		Monitor usage	NO
	Personal data provision	**Block**	NO
	Streaming	**Block** the access	Application - NO
			Web - NO
		Monitor the access to the application	NO
	P2P application	**Block** the application	NO
		Monitor downloads	NO
	Skype application	**Block** (chat, VoIP, Video-chat)	NO
		Monitor the access	NO
		Prevent from *new* contact	NO
	Windows Live Messenger	**Block** the application	NO
		Monitor the access	NO
		Prevent from *new* contact	NO
	e-mail	**Block** email Client and/or web	NO

DETAILED SECURITY FINDINGS

The Tool prevents the user from by-passing the filter by:	YES/NO
Using the IP address instead of the URL	YES
Using an alternative browser	YES
Changing time and date settings*	N/A
Disabling or uninstalling the software without a password*	YES
Closing the filtering tool trough the Task Manager	YES
Using a proxy instead of a direct connection to the internet.	YES
Accessing the web-pages through the Google cache	NO
Reaching a website through translation sites	YES
Renaming a blocked application	N/A
Using Safe Mode	NO
Changing the port of Peer-to-Peer application	N/A

**As managed directly by the tool and not by the device.*

DETAILED USABILITY FINDINGS

	YES/NO
I: installation in 3 steps or less	NO
I: choice of installation for beginners or advanced users	NO
C: different degrees of strength for the filtering	NO
C: different content criteria for the filtering	NO
C: option to transfer filter configurations between target users	No user profiles
C: option to transfer filter configurations between devices	YES
C: altogether comprehensible configuration	NO
C: altogether in conformity with user expectations	NO
C: altogether easy to learn	NO
U: alert message in a child friendly language	YES
U: option to customise the reaction in case of blocking	NO
U: altogether user friendly and comprehensible reporting	No reporting