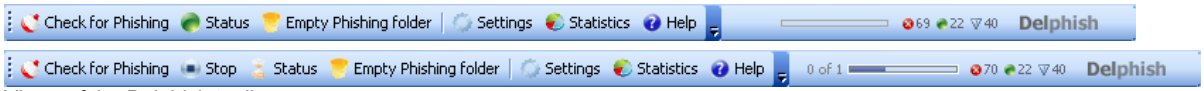
Delphish Help

Version 1.0 Beta 1
August 2006

Table of contents

After the installation of the Delphish Add-In

After the installation, the Delphish toolbar is displayed in MS Outlook. It allows incoming emails to be checked for Phishing, and it provides information and details about emails that were previously checked for Phishing.



Views of the Delphish toolbar

Additionally, the Delphish-Add-In creates a new folder with the name “Phishing” below the Inbox folder of the default mailbox. If that folder exists already, Delphish doesn't create a different one. The existing folder will be used automatically instead.
Emails that are rated as Phishing will be moved into this folder.

Checking an email for Phishing

The following paragraphs explain in simple and easy to follow steps, how you can use Delphish to examine an email for a potential threat through Phishing. The different options will be described in detail.

Choose the email you want to check

You can choose any email to be checked from the Outlook inbox or a subfolder. The following icon appears in the Delphish toolbar, if you select an unchecked email:

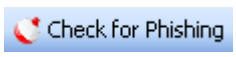
It shows that this email has not previously been examined by Delphish. The status icon can have several other looks. They are described in the section “Viewing the status report”.

You can only choose one email to be checked for Phishing at a time. However it’s possible to initiate the check for the next and further emails, before the check of the first email completes. All emails will then be checked successively.

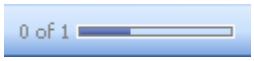
Further information about the Phishing check of multiple emails can be found in the section “Checking multiple emails for Phishing”.

Check the email

To carry out the check, simply click on the button



If the email was checked previously, the status report will be displayed.
In case emails cannot be checked, an error message is displayed. If the email was not previously checked, the Phishing check will start instantly. A progress bar in the Delphish toolbar shows the check status:



The progress bar shows the part of the emails that has been checked already. The status icon also indicates the running check by displaying an hourglass.

The Stop button appears to the left hand side of the status icon. It is only used when checking multiple emails though.

Check result

Three different scenarios can occur when the Phishing check completes:

- The email was recognized as Phishing attempt
- The email could not be rated
- The email was recognized as harmless

Recognized Phishing attempt

If the email contained explicit signs indicating Phishing, the following test report is displayed:

Test report

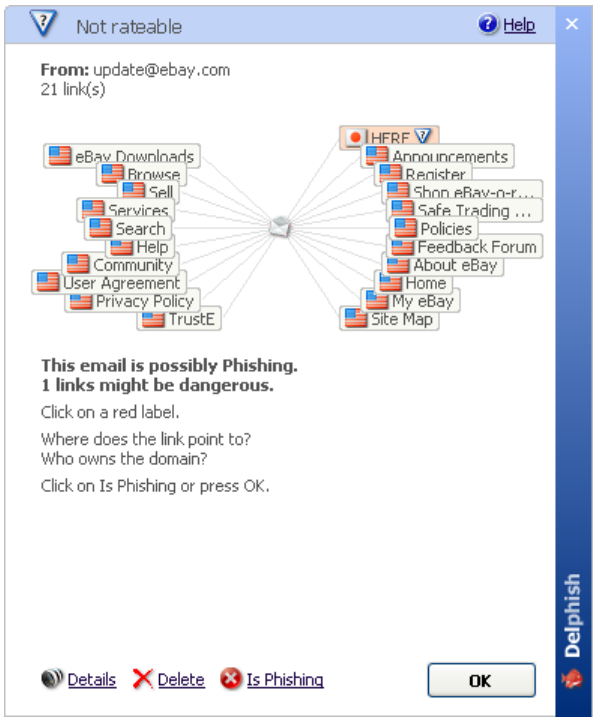
No further information will be displayed automatically. When you close the test report, the Phishing email will be moved to the Phishing folder. The section “Email not rateable” describes how to obtain further details about the checked email. The status report is explained there, which can be opened through the Status button in the Delphish toolbar.

Email not rateable

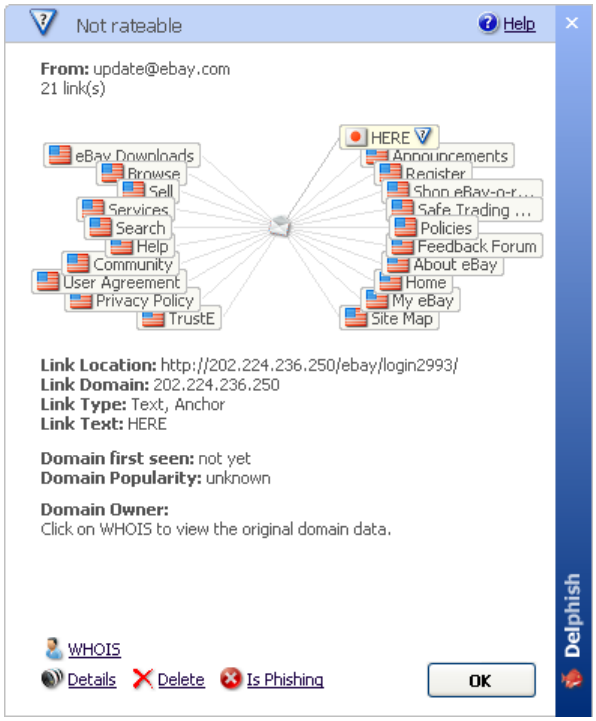
If Delphish cannot rate the email explicitely as “Phishing” or “No Phishing”, the status “Not rateable” is assigned to the email. In this case the test report isn’t displayed. Instead the status report with information about the potential danger from this email is displayed instantly.

Status report is displayed

This information shall help you to determine, whether this email is a Phishing email or not. The view contains the sender of the email as well as all the links of the email in a concise, graphical display. The flags with the text next to them allow for a quick detection of potentially dangerous links. This view shall only provide you with an overview though. Each link reveals more information by clicking on it. The details are then shown below the LinkView instead of the short evaluation.



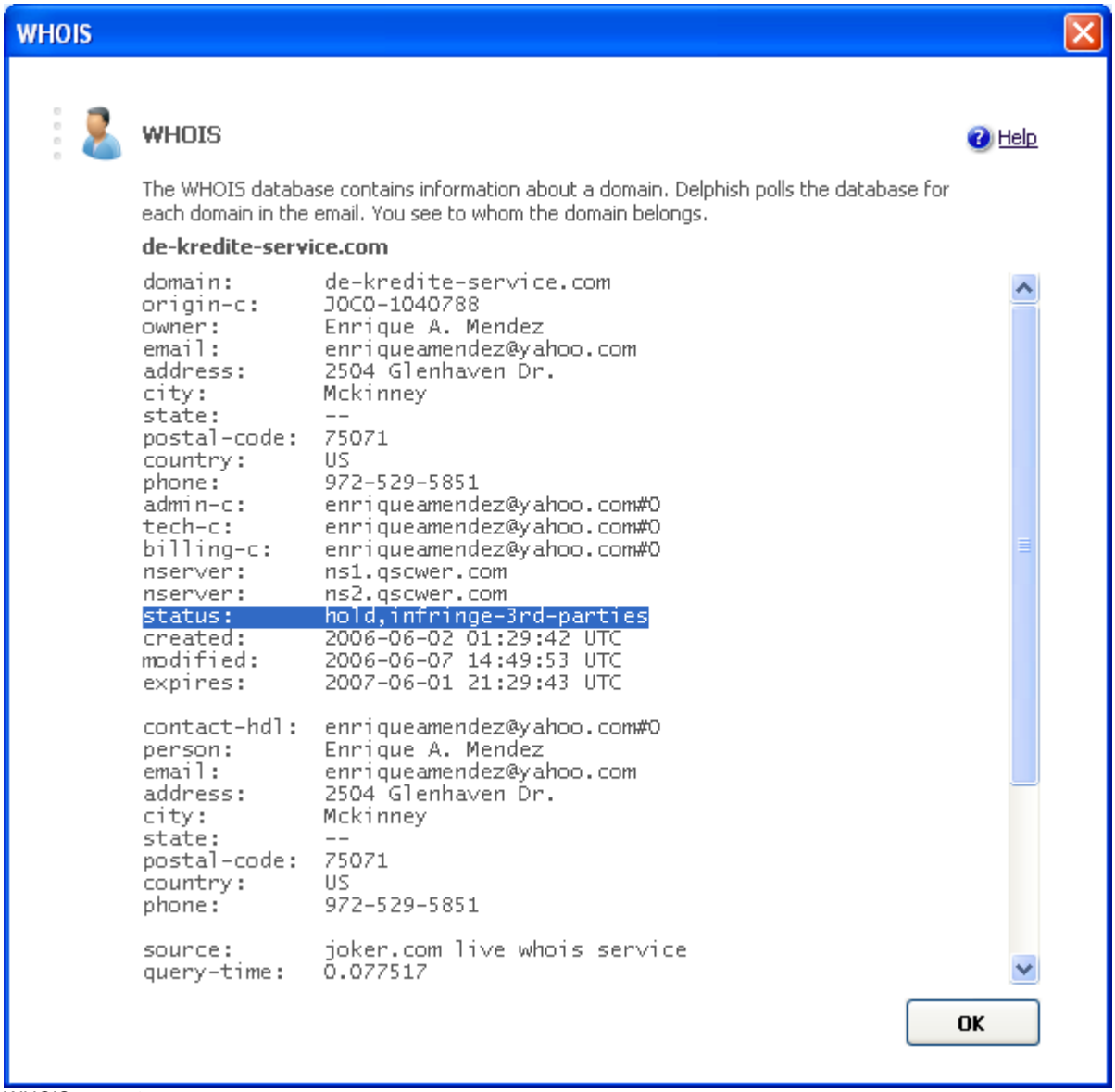
You see the real address of the link, which is always disguised by deceptive descriptions in Phishing emails. The domain name is shown below, so you can see the server that the link points to at a glance. The Link Type specifies the element type that contains the link. That can be a text, a picture or a form but also something potentially dangerous like JavaScript. The Link Text contains, depending on the link type, the text that the user sees in the email, or the description of the linked picture. The link text is arbitrary, which makes it possible to display something completely different than the real link address, e.g. a fake address.



The age of the domain and it’s popularity give you some more hints about the seriousness of the operator. The address of the Domain Owner completes the status report.

WHOIS – Who are you?

The WHOIS (spoken: who is) button in the lower area of the window brings up detailed information about the domain of the selected link.



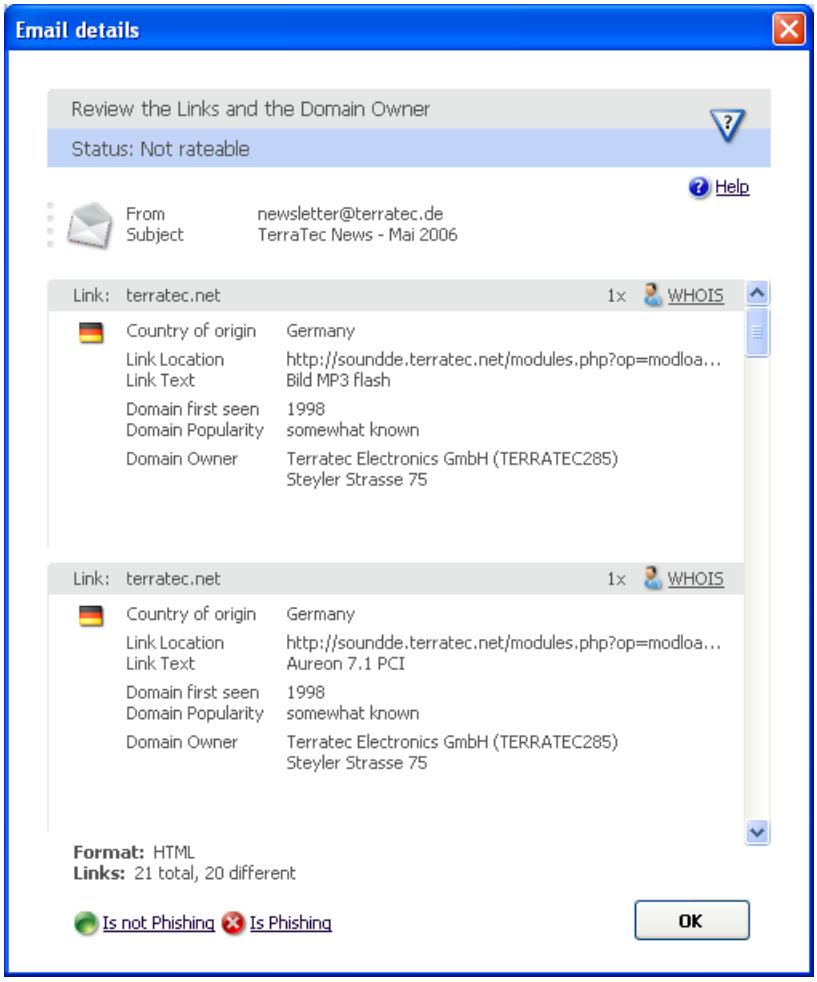
WHOIS request

This is a WHOIS request for a link in a Phishing email. Some more information about the domain can be found here, which can't be explained in-depth since this is beyond the scope of this manual. The status of the domain is highlighted here, because it can also allow conclusions about the seriousness. The status says “hold,infringe-3rd-parties” here, which means that the domain was locked due to the violation of third party rights. This is a definite hint for Phishing, whereas the Phishing threat has already been disabled for this domain because it is locked.

Detailed view of the links

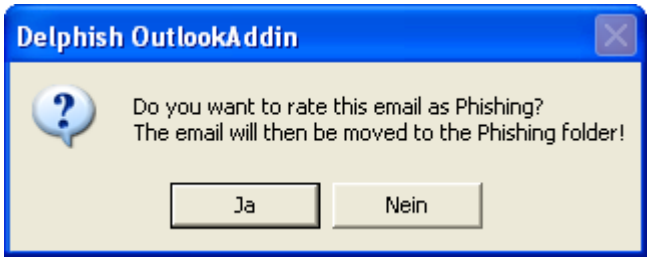
You can bring up a plain text view of the links by clicking the Details button in the status report.

The additional information that is shown in this window are the email subject, the name of the country of origin of each link as well as the number of total and different links. Links are only counted as identical, if the link type, the link text and the link address match. Links with multiple occurrences in the email are marked through the number that is shown next to the WHOIS button.



Rating the email manually

If you want to give the email a specific rating as Phishing or as a normal email, on the basis of the information of the status report, you can do that in the window Email details with the buttons “Is not Phishing” and “Is Phishing”. The option “Is Phishing” is also directly available in the status report. When you choose this option, the moving of the email into the Phishing folder needs to be confirmed in a dialog box.



Delete the email

Finally the status report also directly allows the email to be deleted through the appropriate button. This operation also needs to be confirmed in a dialog box.

The email was recognized as harmless

The status report appears in the following form, if Delphish can explicitly rate the email as “No Phishing”:

Status report “No Phishing”

You can confirm this window with the OK button, because this email is harmless. If you would like to rate this email as Phishing anyway, you can do that by clicking the Phishing button. Alternatively you can delete the email directly by clicking the Delete button. Both options need to be confirmed by dialog boxes. More information about that can be found in the section “Email not rateable”. The Details button is inoperable in this window.

Checking multiple emails for Phishing

You can only choose one email to be checked for Phishing at a time. However it's possible to initiate the check for the next and further emails, before the check of the first email completes. All emails will then be checked successively. The Stop button appears in the Delphish toolbar next to the Status icon with the hourglass.

The hourglass icon of the Status button shows that the currently selected email is currently being checked. If the user selects a different email during the check, the icon of the Status button changes to reflect the status of the currently selected email. The Stop button allows you to abort the Phishing check. The check will be cancelled, after the entire check of the currently processed email completed.

During the check a progress bar in the Delphish toolbar shows the current status of the Phishing check.

A numerical display is located on the right hand side of the progress bar. It shows the total number of recognized emails in the categories "Phishing", "No Phishing" and "Not rateable". This display is updated after every email during the check.

When the check is finished, the test report is displayed with an overview of the checked emails.

Test report

No further information will be displayed automatically. When you close the test report, the Phishing emails will be moved to the Phishing folder. If you want to see further details about one of the checked emails, simply select the email. The status report will show up automatically. Information about the potential dangerousness of the emails can be found in the section "Email not rateable". The status report is explained there, which can be opened through the Status button in the Delphish toolbar. The section "Viewing the status report" contains additional hints about the status report.

Viewing the status report

The status report can be brought up at any time by clicking the Status button in the Delphish toolbar.

The Status button can have the following appearances:

Email is harmless

Email is not rateable

Email is a Phishing email

Email has not been checked yet or no email is selected

Email is being checked

Examples for status reports can be found in the sections “Recognized Phishing attempt”, “Email not rateable” and “The email was recognized as harmless”.

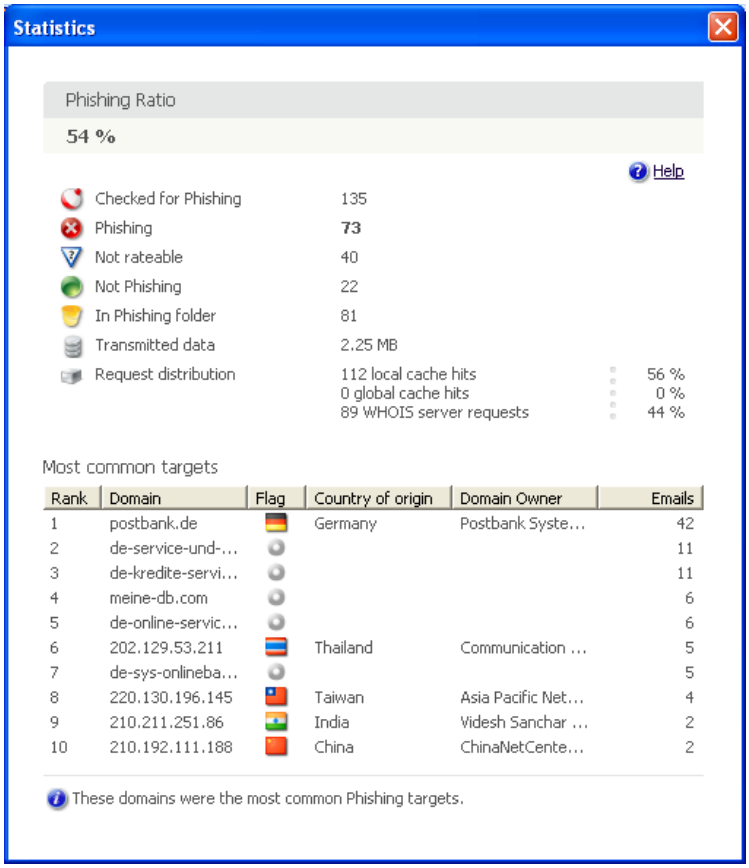
Statistics for Delphish usage

Delphish also offers informative statistics, that shall be briefly explained here.

The number of checked emails with their categories are shown, as well as the corresponding ratio of Phishing emails. The transmitted data is determined by the amount of data that is transferred for obtaining the domain information.

The request distribution relates to the WHOIS (spoken: who is) requests. When a domain is requested for the first time, the data is stored locally so it’s immediately available for a future request of the same domain.

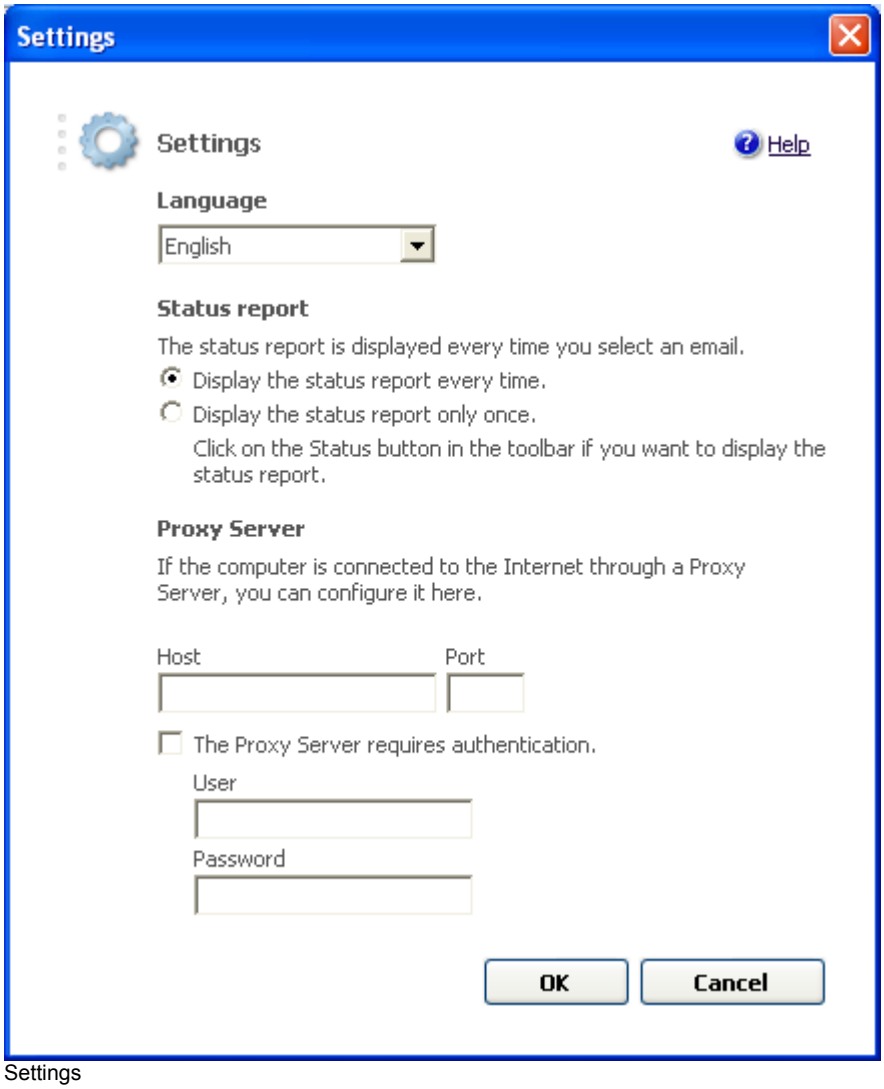
The table with the Most common targets shows you the 10 domains that are linked most frequently in Phishing emails.



Configuring Delphish

Delphish can be configured through the Settings button in the Delphish toolbar.

The options of the Settings window are described below.



Settings

Choose the language

The language can be set conveniently through the drop-down box. The changes take effect immediately after pressing OK. Currently Delphish is available in the languages English and German. The presetting for the language selection is defined through the regional settings of Windows.

Configuring the status report

The status report can be configured to be automatically displayed when an email is selected, or not. The most secure way is to automatically display the status report. That makes sure that you are notified for every email, whether it’s harmless, potentially dangerous or actually dangerous.

The option “Display the status report only once” causes the status report to be displayed only once directly after the check of the email. Choosing the same email again later will only cause the Status icon in the Delphish toolbar to change and reflect the status of the email.

Phishing emails are an exception to this rule. The status report always shows up when Phishing emails are selected. This security measure is for your protection and cannot be deactivated.

Connecting to the internet through a proxy server

If your computer has no direct connection to the internet, the Settings window allows you to set the appropriate values for the proxy server. The configurable data includes the host name of the proxy server and it's port, as well as possibly necessary authentication information.

Reference

1. The Delphish toolbar

The Delphish toolbar contains the following icons and elements:

When you click on the button “Check for Phishing”, the currently selected email will be checked for Phishing, unless the email has been checked before.
If the email was checked previously, the status report will be displayed.
In case the selected email cannot be checked, an error message is displayed.

The Stop button appears only during a check in progress. The check can be cancelled by clicking the Stop button. The check will end after the check of the current email has completed.

Status

The Status icon shows the status of the currently selected email. The different possibilities are:

- Email is being checked

- Email is Phishing

- Email is Not Phishing

- Email is not rateable

- Email has not been checked or no email is selected

When you click on the Status icon, the status report will be displayed.

When you click on the button “Empty Phishing folder”, all emails will be moved from the Phishing folder to the Deleted Items folder. The operation needs to be confirmed in a dialog box.

When you click on the Settings button, the Settings window will be displayed. The Delphish configuration can be adjusted there.

When you click on the Statistics button, the Statistics window will be displayed.

When you click on the Help button, the online help will be opened in your default web browser.

The progress bar shows the progress of the current Phishing check.

The status “1 of 3” means that currently three emails are being checked, and that the check of the first email has already completed.

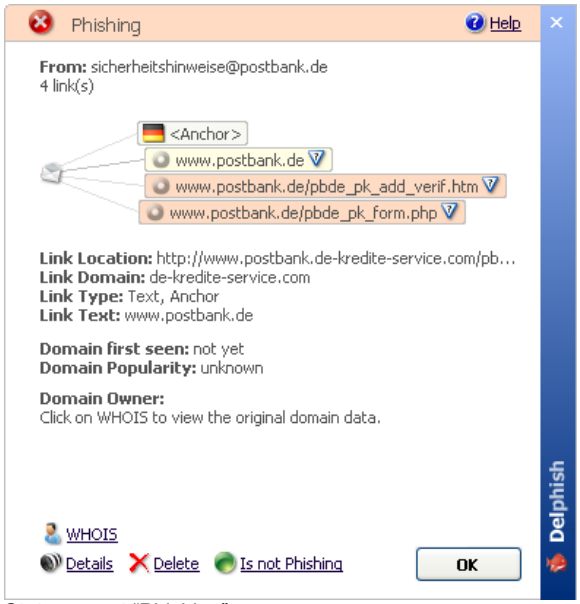
The progress bar fills up while the check progresses.

Three small icons next to the progress bar show the rating of the checked emails. The icons show:

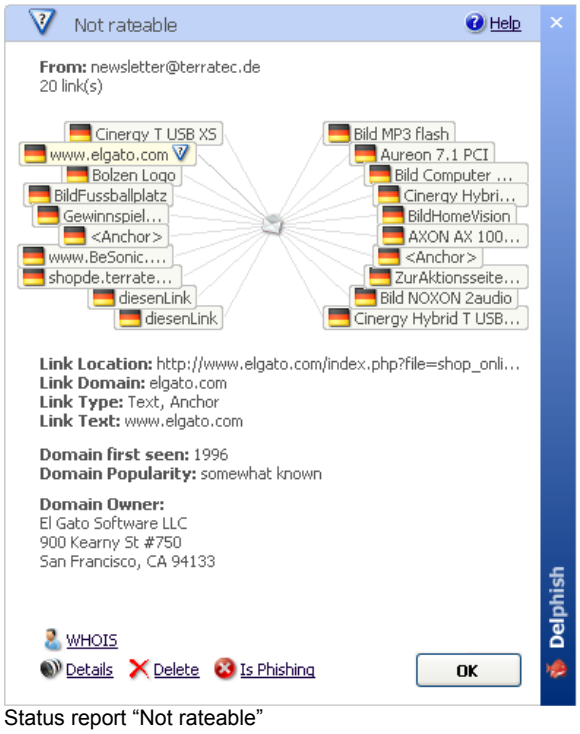
- Phishing
- No Phishing
- Not rateable

When you click on the Delphish logo, the Delphish homepage will be opened in your default web browser.

2. The status report



Status report “Phishing”



Status report “Not rateable”

Status icon and label
shows the status of the currently selected email. Possible status values are “Phishing”, “No Phishing” and “Not rateable”.

From
shows the sender address.

Number of link(s)
displays the number of different links in the email.

LinkView
lists all links in the email circularly. When you click on a link, additional information about the link is displayed. Afterwards you can navigate between the links with the mouse wheel or the cursor keys, or by simply clicking a different link with the left mouse button.

Link Location
shows the location, that the link points to.

Link Domain
shows the domain name, that the link points to.

Link Type
shows the type of the selected link. Possible values are Anchor, Text, Picture, Form, link-sensitive Area and JavaScript.

Link Text
shows the text that the user sees in the email, depending on the link type. In the case of pictures, the title tag or the alt-tag text is displayed.

Domain first seen
shows the year, when the domain was seen on the internet for the first time.

Domain Popularity
shows the level of publicity of the domain.

Domain Owner
shows information about the domain owner, who registered the domain. If this information cannot be obtained, Delphish requests you to click on the WHOIS button. That will open the WHOIS window, where

Status report “No Phishing”

you can see the original WHOIS information.

WHOIS
shows the WHOIS information for the domain that belongs to the selected link.

Details
opens the window Email details. It contains the WHOIS information as text.

Delete
moves the email to the Deleted Items folder. The operation needs to be confirmed in a dialog box.

Is Phishing / Is not Phishing
changes the status of the email and moves emails to the Phishing folder, if they are marked as Phishing.

OK button
closes the status report.

Delphish logo
opens the Delphish homepage in your default web browser.

If multiple emails were successively selected to be checked, or if the checked email is no longer selected when the check completes, a test report is displayed after the check with a summary of the Phishing check.

Test report

The test report shows the number of checked emails and how they were rated.

If errors occurred during the process, the test report shows the number of affected emails.

The test report needs to be closed. Afterwards status reports can be shown and detected Phishing emails will be moved to the Phishing folder.

3. Details

Further information about the checked email can be obtained through the Details button in the status report.

Details

The Email details window will be displayed.

Status
shows the status of the currently selected email. Possible status values are “Phishing”, “No Phishing” and “Not rateable”.

From
shows the sender of the email. This is read from the “From” field of the email header.

Subject
shows the subject line of the email.

Below that, a list of all the links in the email is shown. A scrollbar appears, if the email contains more than two links. The following details are shown for each link:

Link
shows the domain of the link. The number of occurrences of the link in the email is shown at the right hand side in this bar.

WHOIS
leads to the WHOIS information for the domain that belongs to the selected link.

Country of origin
shows the flag and the name of the country of origin.

Link Location
shows the location, that the link points to.

Link Text
shows the text that the user sees in the email, depending on the link type. In the case of pictures, the title tag or the alt-tag text is displayed.

Domain Owner
shows information about the domain owner, who registered the domain.

Format
shows the format of the email. Possible formats are plain-text or HTML.

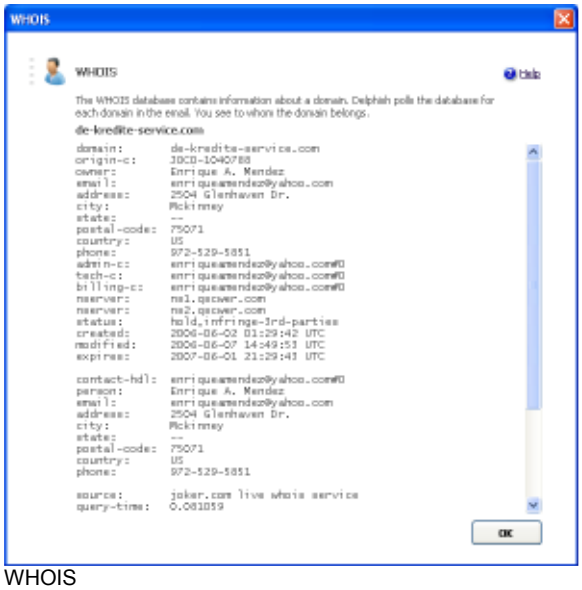
Links
shows the total number of links in the email and the number of different links (in the second case, links with multiple occurrences are only counted 1x).

“Is not Phishing” button
changes the status. The email rating will be “No Phishing”. This button is inactive, if the email is already rated as “No Phishing”.

“Is Phishing” button
changes the status. The email rating will be “Phishing” and it will be moved to the Phishing folder. This button is inactive, if the email is already rated as “Phishing”.

OK button
closes the Email details window.

4. WHOIS Information



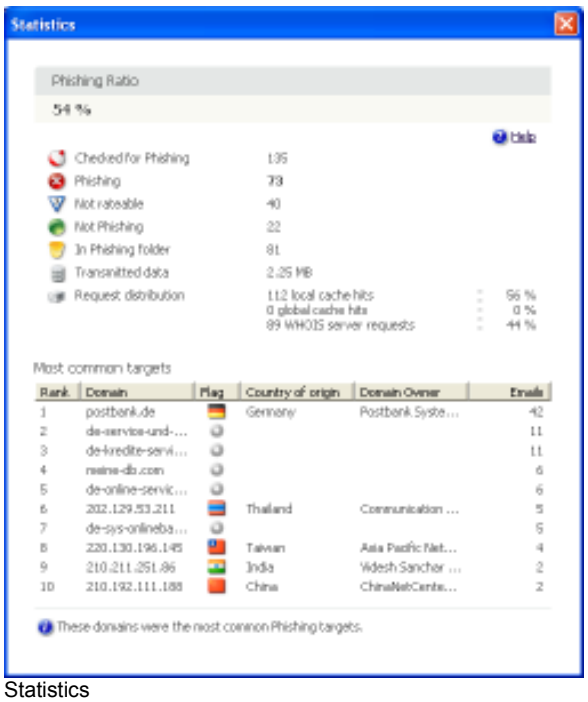
WHOIS

Text field
shows the WHOIS information of the domain that belongs to the link, through which the WHOIS window was opened.

OK button
closes the WHOIS window.

5. Statistics

The results of all checks are evaluated in the statistics window.



Statistics

Phishing Ratio
shows the ratio of the emails rated as Phishing, related to all previously checked emails.

Checked for Phishing
shows the number of checked emails.

Phishing
shows the number of emails that were rated as “Phishing”.

Not rateable
shows the number of emails that could not be rated by Delphish.

Not Phishing
shows the number of emails that were rated as “Not Phishing”.

In Phishing folder
shows the number of emails that are currently in the Phishing folder.

Transmitted data
shows the number of bytes, that were transferred to obtain the domain information.

Request distribution
shows where the displayed WHOIS information came from

- Local cache hit: Shows how often the WHOIS data was obtained from the local database
- Global cache hit: Shows how often the WHOIS data was obtained from the global database
- WHOIS server requests: Shows how often the client made direct WHOIS requests

Most common targets
shows the 10 domains, that were most frequently linked in Phishing emails. Further information about the domains are:

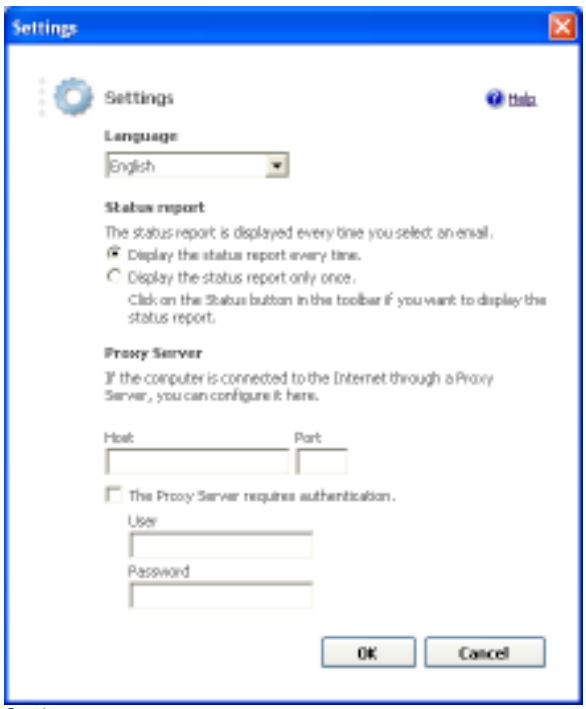
- Rank of the linked domain

(The most frequently linked domain in Phishing emails has the rank 1. The rest is ordered by descending frequency.)

- Domain that the link points to
- Flag of the country with the server that hosts the domain
- Country of origin of the server that hosts the domain
- Domain Owner, who registered the domain
- Number of emails that contained the domain

6. Settings

The settings for the Delphish-Add-In can be configured in the Settings window.



Settings

Language
Here you can change the language of the Add-In

Status report
Here you can specify whether the status report should always be displayed, when a previously checked email is selected, or only once directly after the check completes. This setting has no effect on the emails that are rated as Phishing. The status report automatically shows for those emails.

Proxy Server
Here a proxy server including authentication data can be specified, if the connection to the internet runs through a proxy.