

# Ayuda Delphish

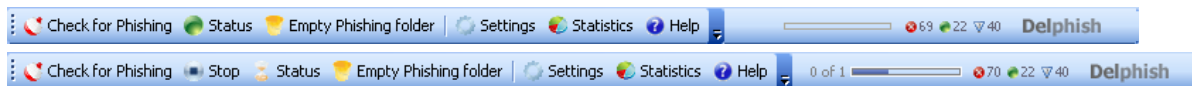
Versión 1.0  
Enero 2007  
Copyright © Nutzwerk GmbH

## Índice

Después de instalar el Add-In Delphish .....	3
Verificar varios e-mails con respecto a phishing .....	3
Realizar la verificación .....	3
Resultado de la verificación .....	4
Detección de un intento de fraude por phishing .....	4
E-mail no clasificable con claridad .....	5
Visualización del informe de estado .....	5
WHOIS – ¿quién eres? .....	6
Vista detallada de los links .....	7
Ejecución manual de la clasificación .....	7
Borrar e-mails .....	8
El e-mail ha sido identificado como inofensivo .....	8
Verificar varios e-mails con respecto a phishing .....	9
Mostrar el informe de estado .....	10
Estadísticas sobre el uso de Delphish .....	10
Configuración de Delphish .....	11
Selección del idioma .....	11
Configurar la visualización del informe de estado .....	12
Conexión con Internet a través de servidor proxy .....	12
Referencia .....	13
1. La barra de herramientas Delphish .....	13
2. El informe de estado .....	15
3. Details (Detalles) .....	17
4. Información WHOIS .....	19
5. Estadística .....	20
6. Configuración .....	22

## Después de instalar el Add-In Delphish

Después de la instalación se muestra en MS Outlook la barra de herramientas Delphish a través de la cual se realiza la verificación de los e-mails entrantes con respecto a phishing, así como la consulta de información y detalles de los e-mails ya verificados con respecto a phishing.



Vistas de la barra de herramientas Delphish

El Add-In Delphish crea además en Outlook, por debajo de la entrada de correo perteneciente a la bandeja estándar, una nueva carpeta con el nombre "Phishing". Si ya existe una carpeta con este nombre, Delphish la utiliza y no crea ninguna nueva. Los e-mails clasificados como phishing se trasladan a esta carpeta.

## Verificar varios e-mails con respecto a phishing

A continuación se explica en pasos sencillos y fáciles de ejecutar la manera de verificar un e-mail con Delphish con respecto a una amenaza potencial por phishing. Se tratan detalladamente las distintas opciones.

### ***Seleccionar un e-mail para su verificación***

Seleccione en la bandeja de entrada de Outlook o una subcarpeta cualquier e-mail que desee verificar. En la barra de herramientas Delphish aparece este icono si no se ha verificado el e-mail en cuestión:



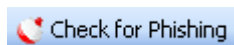
Indica que, hasta este momento, el e-mail en cuestión no ha sido examinado por Delphish. El icono de estado puede tomar otras formas que se describen en el apartado "Mostrar el informe de estado".

Sólo se puede seleccionar un e-mail a la vez para comprobarlo con respecto a phishing. Sin embargo, es posible iniciar la verificación del e-mail siguiente y de otros adicionales antes de que haya finalizado la comprobación. Entonces, la verificación de todos los e-mails se ejecuta sucesivamente.

Más información sobre la comprobación de phishing de varios e-mails figura en el apartado "Verificar varios e-mails con respecto a phishing".

### ***Realizar la verificación***

Para iniciar la verificación basta con hacer clic en el botón



Para e-mails que ya se hayan verificado anteriormente se muestra el informe de estado. Para e-mails que no se pueden comprobar aparece un mensaje de error. Si el e-mail no ha sido verificado hasta la fecha, la comprobación de phishing se inicia inmediatamente y una indicación de avance en la barra de herramientas Delphish informa sobre su desarrollo:



La barra de avance indica la proporción del e-mail que ya se ha verificado. El icono de estado indica igualmente la verificación en curso en forma de un reloj de arena:



A la izquierda del icono de estado aparece el botón Stop. Sin embargo, éste sólo se utiliza cuando se verifican varios e-mails.

## **Resultado de la verificación**

Al finalizar la verificación de phishing se pueden producir tres casos distintos:

- El e-mail ha sido identificado como intento de fraude por phishing
- El e-mail no se ha podido clasificar claramente
- El e-mail ha sido identificado como inocuo

## **Detección de un intento de fraude por phishing**

Si, en el e-mail verificado, se encuentran indicios claros de phishing aparece el siguiente informe de verificación:



Informe de verificación

No se visualiza automáticamente una eventual información adicional. Al cerrar el informe de verificación, el e-mail de phishing se desplaza a la carpeta Phishing. La manera de consultar más detalles sobre el e-mail verificado se describe en el apartado "E-mail no clasificable con claridad". Allí se describe el informe de estado que se puede visualizar pulsando el botón Status (Estado) en la barra de herramientas Delphish.

## E-mail no clasificable con claridad

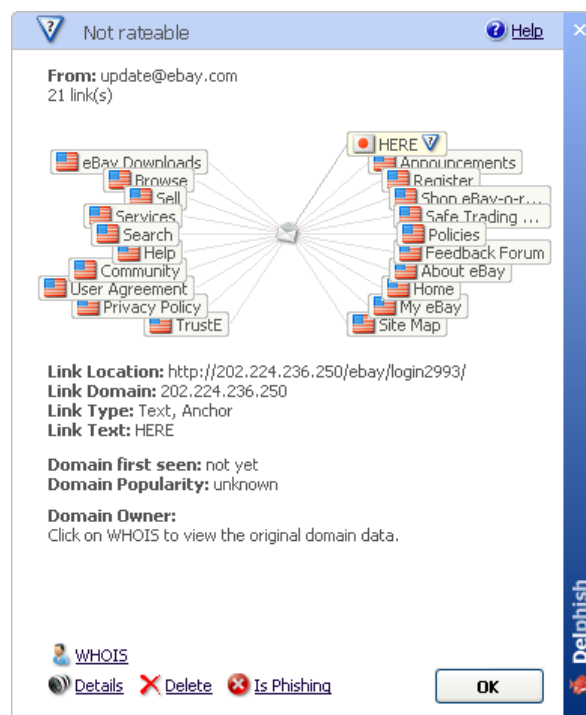
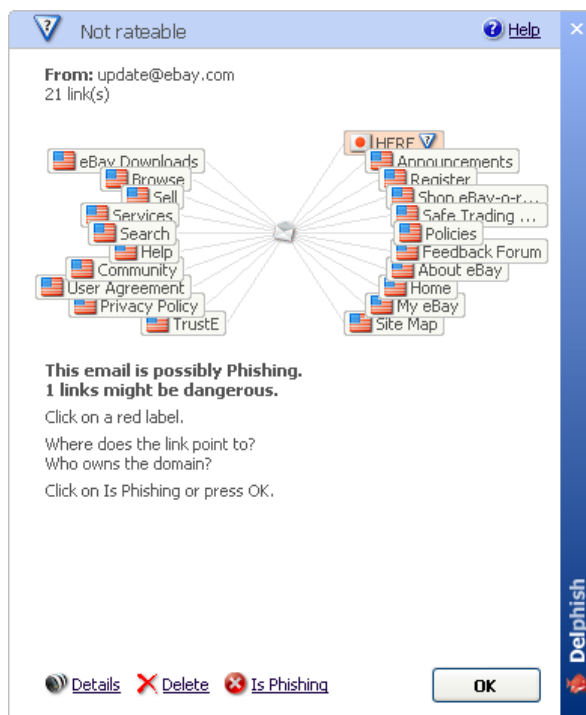
Si Delphish no puede clasificar el e-mail claramente como "Phishing" o "No phishing", el e-mail recibe el estado "No clasificable". En este caso se renuncia a visualizar el informe de prueba; en su lugar, se abre inmediatamente el informe de estado con información sobre el potencial de peligro del e-mail.

### Visualización del informe de estado

Esta información le ayudará a averiguar si este e-mail es un intento de phishing o no. La representación contiene el remitente del e-mail, así como todos los links contenidos en el mismo en una visualización gráfica claramente dispuesta. Mediante las banderas de países y el texto del link que figura al lado se pueden reconocer rápidamente los links potencialmente peligrosos. Sin embargo, de este modo sólo se pretende ofrecer una vista de conjunto. Cada link revela, tras hacer clic en su nombre, más información que aparece en lugar de la evaluación resumida por debajo del gráfico.

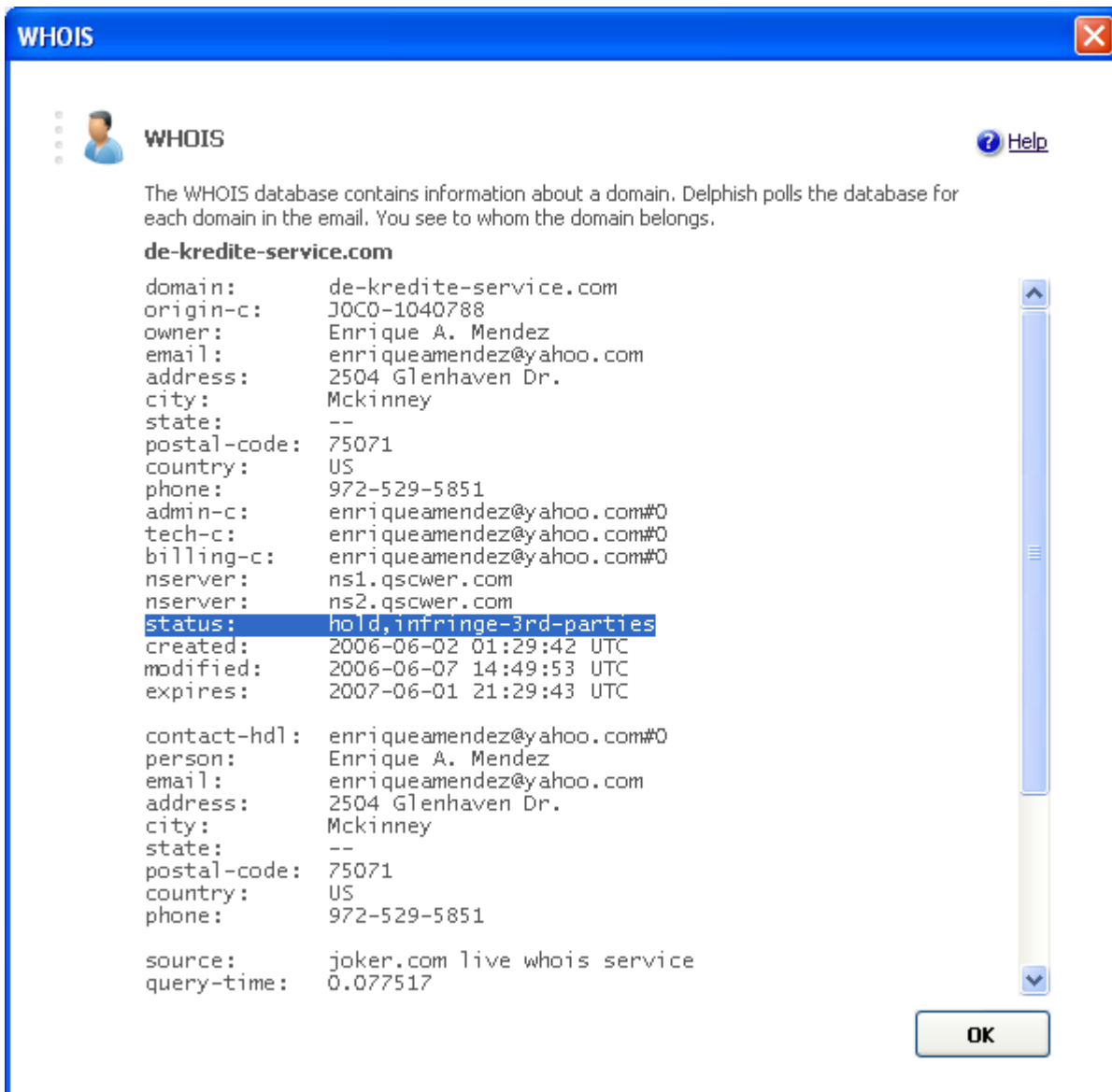
Allí se puede ver la dirección real del link que, en los e-mails de phishing, queda oculta siempre por denominaciones engañosas. A continuación puede ver el nombre del dominio que le permite averiguar en un solo vistazo a qué servidor conduce el link. El tipo de link indica detrás de qué elemento se oculta el link. Puede ser un texto, una imagen o un formulario, pero también algo potencialmente más peligroso como JavaScript. El texto del link contiene, en función del tipo de link, el texto que puede ver el usuario en el e-mail, o bien la descripción de la imagen enlazada. El texto del link se puede elegir libremente, de modo que es posible mostrar algo totalmente distinto a la dirección real del link, por ejemplo una dirección falsificada.

La antigüedad del dominio y su popularidad ofrecen más indicios sobre la seriedad del titular. La dirección del propietario del dominio completa el informe de estado.



## WHOIS – ¿quién eres?

A través del botón WHOIS (pronunciado: who is) en la parte inferior de la ventana se puede consultar información detallada sobre el dominio del link seleccionado.



The screenshot shows a window titled "WHOIS" with a blue header and a red close button. The window contains a list of domain information for "de-kredite-service.com". The status field is highlighted in blue and contains the text "hold, infringe-3rd-parties".

```
WHOIS

The WHOIS database contains information about a domain. Delphish polls the database for
each domain in the email. You see to whom the domain belongs.

de-kredite-service.com

domain:          de-kredite-service.com
origin-c:        J0C0-1040788
owner:           Enrique A. Mendez
email:           enriqueamendez@yahoo.com
address:         2504 Glenhaven Dr.
city:            Mckinney
state:           --
postal-code:    75071
country:         US
phone:           972-529-5851
admin-c:         enriqueamendez@yahoo.com#0
tech-c:          enriqueamendez@yahoo.com#0
billing-c:       enriqueamendez@yahoo.com#0
nserver:         ns1.qscwer.com
nserver:         ns2.qscwer.com
status:          hold, infringe-3rd-parties
created:         2006-06-02 01:29:42 UTC
modified:        2006-06-07 14:49:53 UTC
expires:         2007-06-01 21:29:43 UTC

contact-hdl:    enriqueamendez@yahoo.com#0
person:         Enrique A. Mendez
email:          enriqueamendez@yahoo.com
address:        2504 Glenhaven Dr.
city:           Mckinney
state:          --
postal-code:    75071
country:        US
phone:          972-529-5851

source:         joker.com live whois service
query-time:     0.077517
```

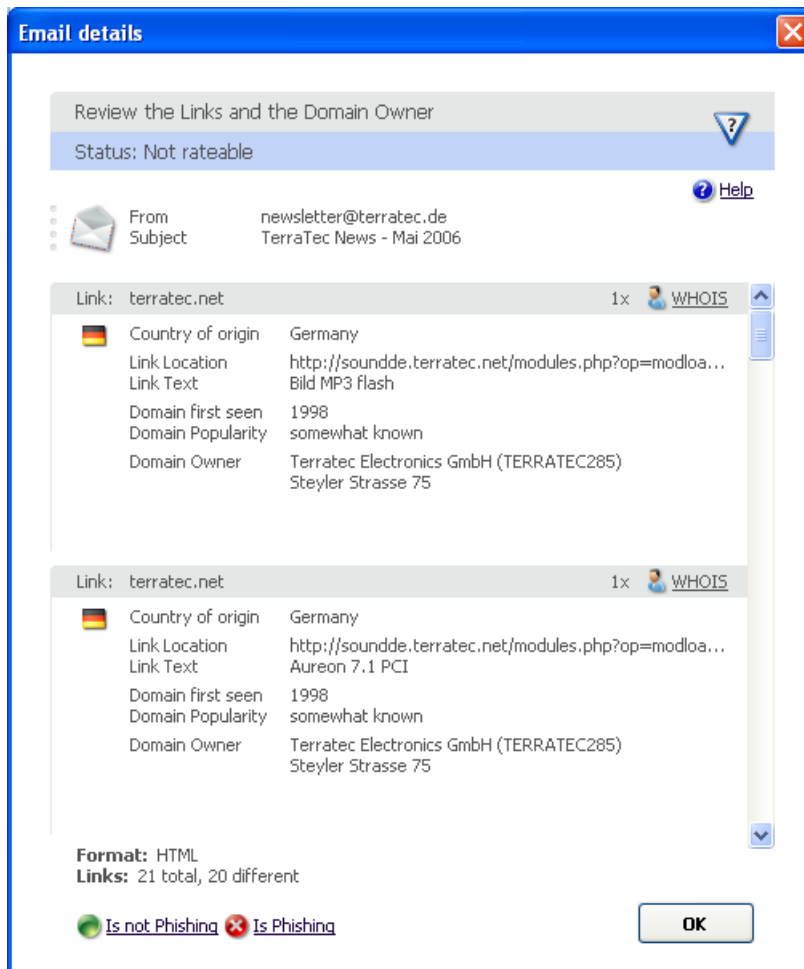
Consulta WHOIS

Ésta es una consulta WHOIS de un link en un e-mail de phishing. Allí se encuentra alguna información adicional sobre el dominio cuya explicación exhaustiva sobrepasaría el marco de esta descripción. El estado del dominio queda resaltado, dado que puede permitir, en su caso, conclusiones sobre la seriedad. El estado se encuentra en "hold, infringe-3rd-parties", lo cual significa que el dominio ha quedado bloqueado debido a la vulneración de derechos de terceros. Ésta es una indicación clara al phishing, aunque el peligro de phishing en este link ya está eliminado gracias al bloqueo del dominio.

## Vista detallada de los links

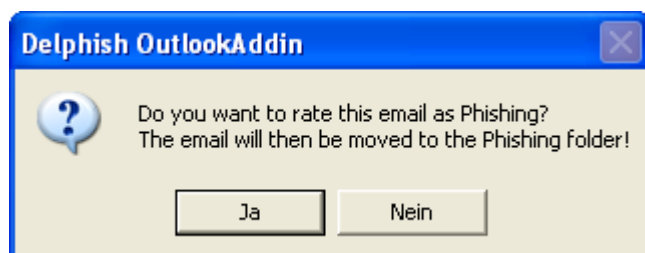
En el informe de estado se puede consultar una representación "sólo texto" del link, pulsando el botón Details (Detalles).

Los datos adicionales que se representan en esta ventana son el asunto del e-mail, el nombre del país de cada link, el formato del e-mail, así como el número total de links y el número de links diferentes. Los links sólo se consideran idénticos si coinciden el tipo, el texto y la dirección del link. Los links que aparecen varias veces en el e-mail se marcan aquí con un número junto al botón WHOIS.



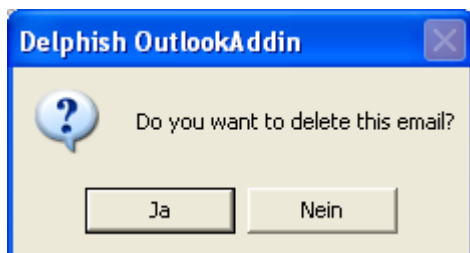
## Ejecución manual de la clasificación

Si quiere realizar en base a la información del informe de estado una clasificación clara del e-mail como phishing o como e-mail normal, puede hacerlo en la ventana Details (Detalles) con los botones "Is not Phishing" (No es phishing) y "Is Phishing" (Es phishing). La opción "Is Phishing" también está disponible directamente en el informe de estado. Si selecciona esta opción tiene que confirmar el desplazamiento del e-mail a la carpeta Phishing en una consulta de seguridad.



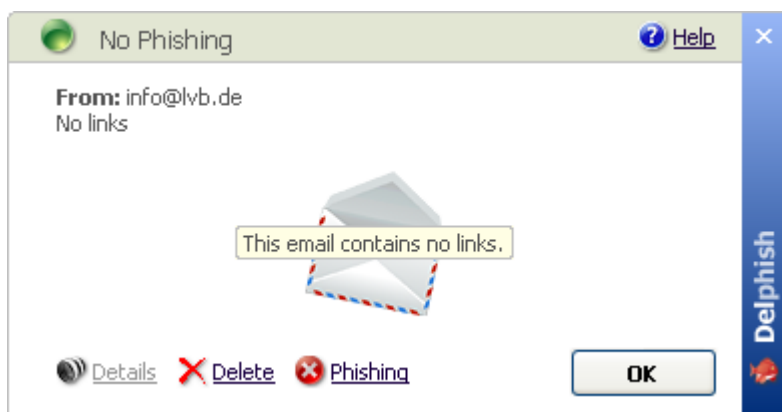
## Borrar e-mails

Finalmente, el informe de estado permite borrar directamente los e-mails a través del botón correspondiente. Este proceso se tiene que confirmar igualmente en una consulta de seguridad.



## El e-mail ha sido identificado como inofensivo

Si Delphish puede clasificar claramente un e-mail en la categoría "No phishing", el informe de estado aparece en esta forma:



Informe de estado "No phishing"

Esta ventana se puede confirmar tranquilamente con OK. Si, a pesar de todo, deseara clasificar el e-mail en cuestión como phishing, dispone del botón Phishing. Como alternativa, el e-mail también se puede borrar directamente con el botón Löschen (Borrar). Ambas opciones se tienen que confirmar con consultas de seguridad. Ver al respecto las descripciones en el apartado "E-mail no clasificable con claridad". En esta ventana, el botón Details (Detalles) está sin función.



## Verificar varios e-mails con respecto a phishing

Sólo se puede seleccionar un e-mail a la vez para comprobarlo con respecto a phishing. Sin embargo, es posible iniciar la verificación del e-mail siguiente y de otros adicionales antes de que haya finalizado la comprobación. Entonces, la verificación de todos los e-mails se ejecuta sucesivamente. En la barra de herramientas, el botón Stop aparece junto al icono de estado con el reloj de arena.



El botón Status (Estado) indica a través del reloj de arena que el e-mail actualmente seleccionado se está verificando. Si el usuario selecciona otro e-mail durante la verificación, se encuentra allí un símbolo que refleja el estado del e-mail seleccionado actualmente. El botón Stop permite cancelar la comprobación de phishing. La cancelación tiene lugar una vez que haya finalizado la verificación completa del e-mail procesado actualmente por Delphish.

Durante la verificación, una indicación de avance en la barra de herramientas Delphish informa sobre el estado actual del proceso.



A su derecha se encuentra una indicación numérica con el número total de e-mails clasificados hasta este momento en las categorías "Phishing", "No phishing" y "No clasificable". Ésta se actualiza durante la verificación después de cada e-mail procesado.



Una vez finalizada la verificación, se muestra el informe de verificación con el resumen de los e-mails verificados.








Informe de verificación

No se visualiza automáticamente una eventual información adicional. Al cerrar el informe de verificación, los e-mails de phishing se desplazan a la carpeta Phishing. Para consultar más detalles sobre uno de los e-mails verificados basta con seleccionarlo. Entonces se muestra automáticamente el informe de estado. Información sobre la evaluación de la peligrosidad de los e-mails figura en el apartado "E-mail no clasificable con claridad". Allí se describe el informe de estado que se puede visualizar pulsando el botón Status (Estado) en la barra de herramientas Delphish. Las indicaciones adicionales sobre el informe de estado se encuentran en el apartado "Mostrar el informe de estado".

## Mostrar el informe de estado

El informe de estado se puede consultar en todo momento pulsando el botón Status (Estado) en la barra de herramientas Delphish.

El botón Status (Estado) puede tomar las siguientes formas:

	El e-mail es inofensivo
	El e-mail no se puede clasificar
	El e-mail es un intento de phishing
	El e-mail no ha sido verificado todavía o no está seleccionado ningún e-mail
	El e-mail se está verificando en este momento

Ejemplos de informes de estado se encuentran en los apartados "Detección de un intento de fraude por phishing", "E-mail no clasificable con claridad" y "El e-mail ha sido identificado como inofensivo".

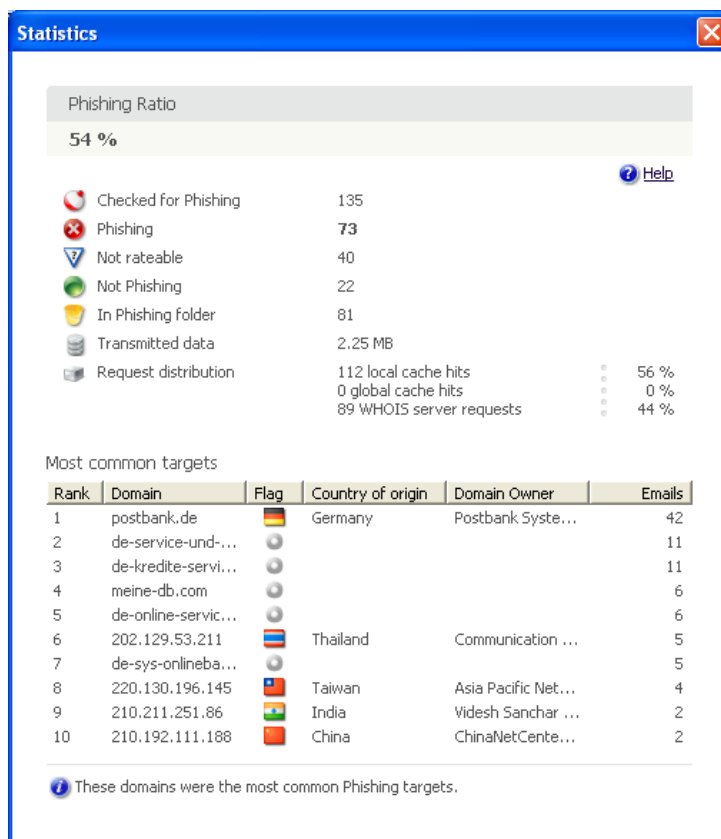
## Estadísticas sobre el uso de Delphish

Delphish ofrece también unas estadísticas informativas que se explicarán brevemente a continuación.

Se indican el número de e-mails verificados, así como su clasificación, al igual que la proporción resultante de e-mails de phishing. El volumen de datos visualizado resulta de la información transmitida para la determinación de la información sobre los dominios.

La distribución de las consultas se refiere a las consultas WHOIS (pronunciado: who is). La primera vez que se consulta un dominio, los datos se guardan a nivel local, con lo cual están disponibles de forma inmediata en la consulta siguiente.

El área Destinos más frecuentes informa con sólo un vistazo de los 10 dominios enlazados con mayor frecuencia en e-mails de phishing.

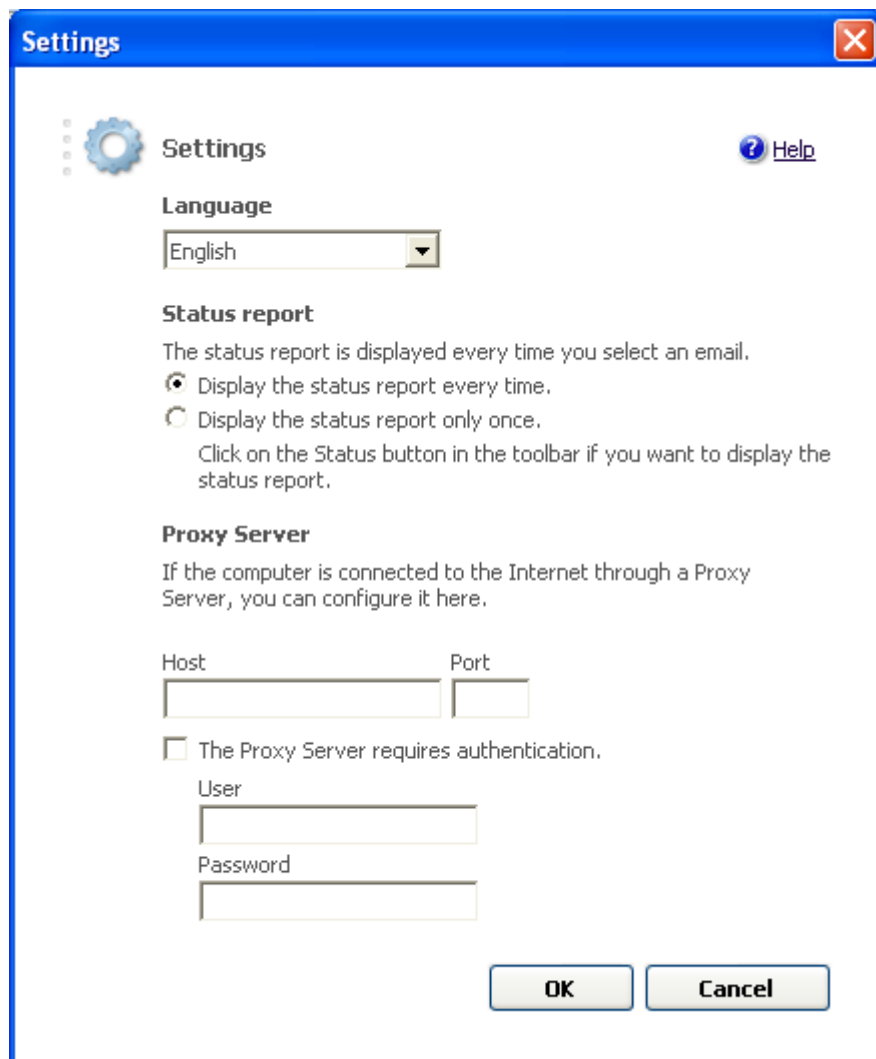


## Configuración de Delphish

La configuración de Delphish se realiza a través del botón Settings (Configuración) en la barra de herramientas Delphish.



A continuación, se explicarán las posibilidades que se ofrecen en la ventana Settings (Configuración).



Configuración

### **Selección del idioma**

El idioma se puede ajustar cómodamente a través del campo de selección. Los cambios se activan inmediatamente después de su confirmación con OK. Actualmente, Delphish está disponible en alemán e inglés. El ajuste previo para la selección del idioma resulta del ajuste local de Windows.

### ***Configurar la visualización del informe de estado***

En el área Informe de estado puede definir si, al seleccionar un e-mail, el informe de estado se visualizará automáticamente o no. La variante más segura es la visualización automática. De este modo, se le informa al seleccionar cualquier e-mail de forma imposible de ignorar si éste es inofensivo, potencialmente peligroso o realmente peligroso.

Si se selecciona la opción " Display the status report only once" (Mostrar el informe de estado sólo una vez), el informe de estado sólo se visualiza después de la primera verificación del e-mail. Si el mismo e-mail se vuelve a seleccionar posteriormente, tan sólo el icono de estado en la barra de herramientas Delphish informa sobre el potencial de peligro del e-mail.

Una excepción son los e-mails de phishing en los cuales el informe de estado se visualiza siempre automáticamente. Se trata de una medida de seguridad que no se puede desactivar para garantizar su seguridad.

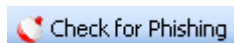
### ***Conexión con Internet a través de servidor proxy***

En el área Proxy Server se pueden realizar los ajustes correspondientes si su ordenador no dispone de un acceso directo a Internet. El nombre de host del servidor proxy con el puerto correspondiente, así como los eventuales datos de usuario necesarios se pueden configurar allí.

## Referencia

### 1. La barra de herramientas Delphish

La barra de herramientas Delphish contiene los siguientes símbolos y elementos:



Al pulsar el botón "Check for Phishing" (Examinar con respecto a phishing), el e-mail seleccionado actualmente se verifica con respecto a phishing si no se ha hecho ya con anterioridad. Para e-mails que ya se hayan verificado anteriormente se muestra el informe de estado.

Si un e-mail seleccionado no se puede verificar, aparece un mensaje de error.



El botón Stop aparece únicamente mientras esté en curso una verificación. La verificación se puede cancelar con "Stop". Entonces termina tras la verificación del e-mail que está siendo procesado en este momento.

Status (Estado)

El símbolo de estado indica el estado del e-mail seleccionado actualmente. Los símbolos de estado posibles son:



Status

- El e-mail se está verificando en este momento



Status

- El e-mail es phishing



Status

- El e-mail no es phishing



Status

- El e-mail no se puede clasificar



Status

- El e-mail no ha sido verificado todavía o no se ha seleccionado ningún e-mail

Al hacer clic en el símbolo de estado se muestra el informe de estado.

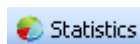


Al hacer clic en el botón "Empty Phishing folder" (Vaciar carpeta Phishing), todos los e-mails de la carpeta Phishing se desplazan a la papelera de reciclaje. Este proceso se tiene que confirmar con una consulta de seguridad.



Settings

Al hacer clic en el botón Settings (Configuración) se abre la ventana Configuración en la cual se puede configurar Delphish.



Statistics

Al hacer clic en el botón Statistics (Estadística) se abre la ventana Estadística.



Help

Al hacer clic en el botón Help (Ayuda) se abre la ayuda online en el navegador de web.



La barra de avance indica el estado de la verificación actual.

La indicación "1 de 3" significa que, en este momento, se están comprobando tres e-mails y la verificación del primer e-mail ya ha finalizado.

La barra de avance se va llenando al avanzar la verificación.



Tres pequeños iconos junto a la barra de avance indican la clasificación de los e-mails verificados. Se muestran:

- Phishing
- No Phishing
- No clasificable

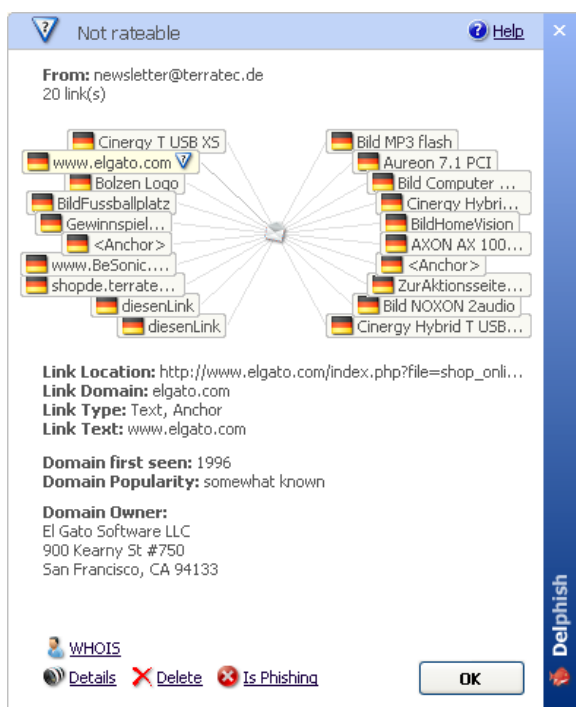


Al hacer clic en el logotipo Delphish se abre la página de inicio Delphish en el navegador de Internet.

## 2. El informe de estado



Informe de estado "Phishing"



Informe de estado "No clasificable"

### Icono de estado y rotulación

indica el estado del e-mail seleccionado actualmente. Los estados posibles son "Phishing", "No phishing" y "No clasificable".

### From (De)

muestra la dirección del remitente.

### Número de links

indica el número de links distintos contenidos en el e-mail.

### LinkView

lista en forma de círculo todos los links contenidos en el e-mail. Al hacer clic en un link se visualiza información adicional sobre el mismo. A continuación, es posible navegar entre los links mediante la ruedecilla del ratón o las teclas de dirección o haciendo clic con el botón izquierdo del ratón.

### Link Location (Dirección del link)

muestra la dirección a la cual apunta el link seleccionado.

### Link Domain (Dominio del link)

muestra el nombre de dominio al cual apunta el link seleccionado.

### Link Type (Tipo de link)

muestra el tipo del link seleccionado. Los datos posibles son Anchor (ancla), Text (texto), Picture (imagen), Form (formulario), link-sensitive Area (área) y JavaScript.

### Link Text (Texto del link)

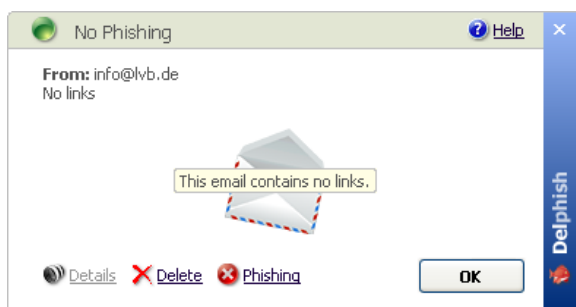
muestra, en función del tipo de link, el texto que puede ver el usuario en el e-mail. En imágenes se muestra el texto Title-Tag o el Alt-Tag.

### Domain first seen (Dominio visto por primera vez)

muestra el año en el cual el dominio fue visto por primera vez en Internet.

### Domain Popularity (Popularidad del dominio)

muestra el grado de popularidad del dominio.



Informe de estado "No phishing"

**Domain Owner (Titular del dominio)**

muestra información sobre el titular que hizo registrar el dominio. Si no es posible determinar estos datos, puede pulsar el botón WHOIS. Entonces se abre la ventana WHOIS en la cual se muestra la información original de WHOIS.

**WHOIS**

muestra la información WHOIS para el dominio que corresponde al link seleccionado.

**Details (Detalles)**

abre una ventana detallada que contiene la información WHOIS claramente estructurada en forma de texto.

**Delete (Borrar)**

desplaza el e-mail a la papelera de reciclaje. Este proceso se tiene que confirmar con una consulta de seguridad.

**Is Phishing / Is not Phishing  
(Es phishing / No es phishing)**

modifica el estado del e-mail y desplaza los e-mails clasificados como phishing a la carpeta Phishing.

**Botón OK**

cierra el informe de estado.

**Logotipo Delphish**

abre la página de inicio Delphish en el navegador de Internet.

Si se han seleccionado sucesivamente varios e-mails para su verificación, o si el e-mail comprobado ya no está seleccionado después de la verificación, aparece al final un informe de verificación con un resumen de la comprobación realizada.



Informe de verificación

Si se han producido errores durante el procesamiento, el informe de verificación indica cuántos e-mails afectan.

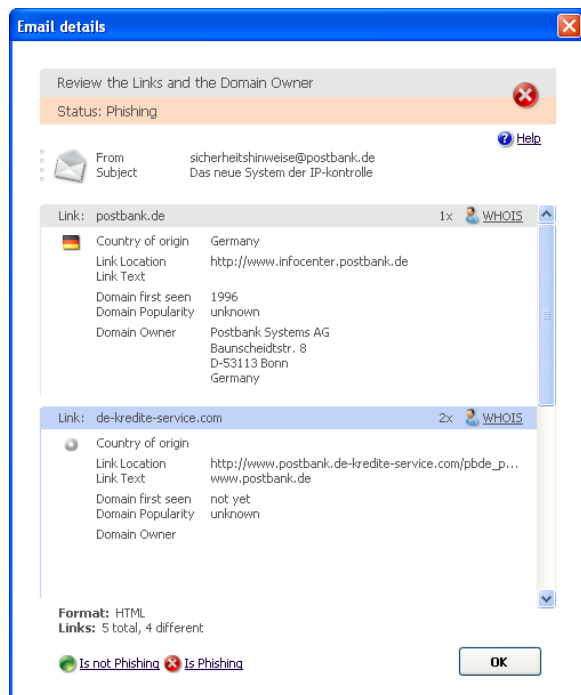
El informe de verificación se tiene que cerrar.

Sólo después se muestran informes de estado y los e-mails identificados como phishing se desplazan a la carpeta Phishing.



### 3. Details (Detalles)

Más información sobre el e-mail verificado se puede consultar pulsando el botón Details (Detalles) en el informe de estado.



Details (Detalles)

Se abre la ventana Email Details (Detalles del e-mail).

#### **Status (Estado)**

indica el estado del e-mail seleccionado actualmente. Los estados posibles son "Phishing", "No phishing" y "No clasificable".

#### **From (De)**

muestra el remitente del e-mail que figura en el campo "From" (de) del encabezamiento del e-mail.

#### **Subject (Asunto)**

muestra la línea de asunto del e-mail.

Debajo se listan todos los links contenidos en el e-mail. Si existen más de dos links aparece una barra de desplazamiento. Para cada link se muestran los siguientes datos:

#### **Link**

muestra el dominio del link. En esta barra aparece a la derecha el número de veces que aparece el link en el e-mail.

#### **WHOIS**

conduce a la información WHOIS para el dominio que corresponde al link.

#### **Country of origin (País de origen)**

muestra la bandera y el nombre del país de origen.

#### **Link Location (Dirección del link)**

muestra la dirección a la cual conduce el link.

#### **Link Text (Texto del link)**

depende del tipo de link y muestra el texto que puede ver el usuario en el e-mail. En imágenes se muestra el texto Title-Tag o el Alt-Tag.

#### **Domain Owner (Titular dominio)**

muestra información sobre el titular que hizo registrar el dominio.

**Format (Formato)**

muestra el formato del e-mail. Los formatos posibles son Plain-Text o HTML.

**Links**

indica el total de links que contiene el e-mail y cuántos links diferentes aparecen (en el segundo caso, los links que aparecen varias veces sólo se cuentan una vez).

**Botón "Is not Phishing" (No es phishing)**

modifica el estado. El e-mail se clasifica como "No phishing". Este botón no está activo si el e-mail ya está clasificado como "No phishing".

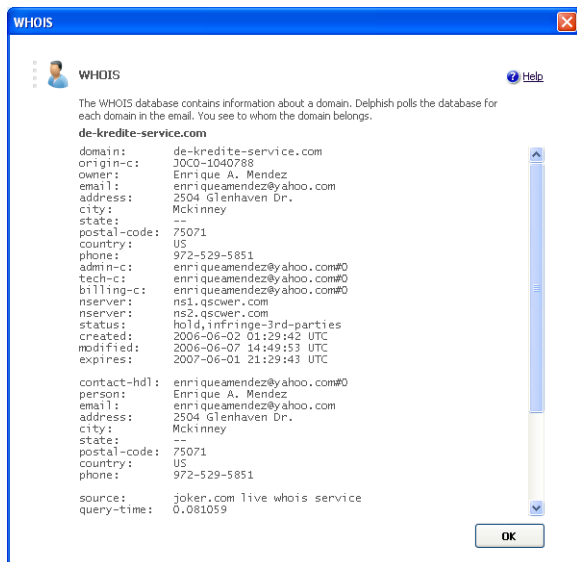
**Botón "Is Phishing" (Es phishing)**

modifica el estado. El e-mail se clasifica como "Phishing" y se desplaza a la carpeta Phishing. Este botón no está activo si el e-mail ya está clasificado como "Phishing".

**Botón OK**

cierra la ventana Details (Detalles).

## 4. Información WHOIS



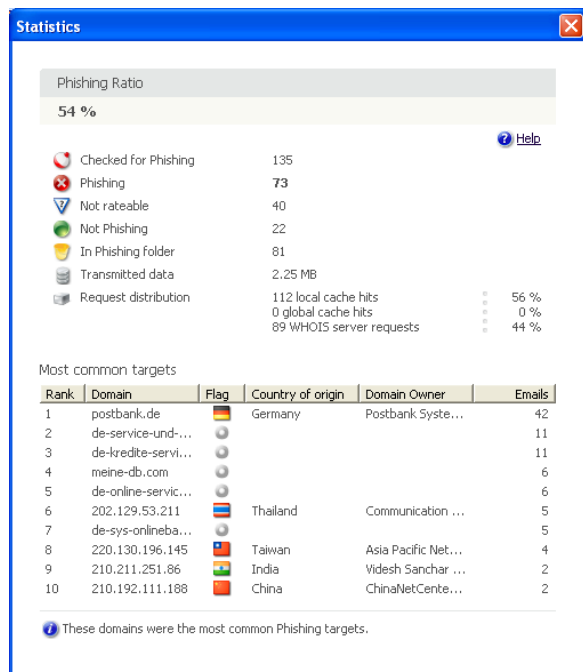
WHOIS

**Text field Campo de texto)**  
muestra la información WHOIS del dominio correspondiente al link a través del cual se abrió la ventana WHOIS.

**Botón OK**  
cierra la ventana WHOIS.

## 5. Estadística

En la estadística se evalúan los resultados de todas las comprobaciones realizadas.



Estadística

**Phishing Ratio (Proporción de phishing)** muestra la proporción de los e-mails clasificados como phishing, relativa a la totalidad de los e-mails verificados.

**Checked for Phishing (Verificado con respecto a phishing)** muestra el número de e-mails que ya han sido verificados.

**Phishing** muestra el número de e-mails clasificados como "Phishing".

**Not rateable (No clasificable)** muestra el número de e-mails que no pudieron ser clasificados por Delphish.

**Not Phishing (No phishing)** muestra el número de e-mails clasificados como "No phishing".

**In Phishing folder (En la carpeta Phishing)** muestra el número de e-mails que se encuentran actualmente en la carpeta Phishing.

**Transmitted data (Volumen de datos)** indica el número de bytes enviados para determinar la información del dominio.

**Request distribution (Distribución de las consultas)** indica de dónde procede la información WHOIS visualizada:

- Local cache hit (Coincidencias caché local): número de datos WHOIS utilizados de la base de datos local
- Global cache hit (Coincidencias caché global): número de datos WHOIS utilizados de la base de datos del servidor
- WHOIS server requests (Consultas servidor WHOIS): número de consultas WHOIS emitidas por el

cliente

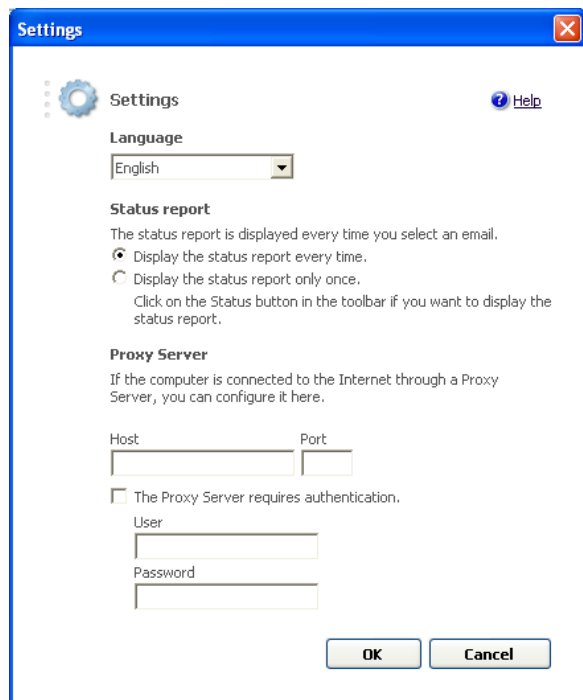
**Most common targets (Destinos más frecuentes)**

muestra los 10 dominios enlazados con mayor frecuencia en e-mails de phishing. Más información sobre este dominio:

- Rango del dominio enlazado (El dominio enlazado con mayor frecuencia en e-mails de phishing tiene el rango 1. El resto se clasifica en orden descendente por su frecuencia.)
- Dominio con el cual se enlaza
- Bandera del país en el cual se encuentra el servidor donde se aloja el dominio
- País de origen en el cual se encuentra el servidor donde se aloja el dominio
- Titular que hizo registrar el dominio
- Número de e-mails de phishing en los cuales se encontró el dominio

## 6. Configuración

En settings (Configuración) se pueden modificar los ajustes del Add-In Delphish.



Configuración

### Language (Idioma)

Aquí se puede seleccionar el idioma del Add-In.

### Status report (Informe de estado)

Aquí se puede ajustar si el informe de estado se mostrará siempre cuando se encuentre seleccionado un e-mail que ya haya sido verificado, o sólo una vez directamente al finalizar la verificación. Este ajuste no influye en los e-mails clasificados como phishing. En estos e-mails, el informe de estado se visualiza en todo caso.

### Proxy Server (Servidor proxy)

Aquí se puede indicar un servidor proxy con datos de autenticación si el acceso a Internet pasa por un proxy.