Vade Secure
Office 365

Vade Secure for Office 365

Contents

Getting started

Dear user,

We are setting up a new security solution to protect your messaging platform. This solution will allow you to find in your inbox only the legitimate messages you'd like to see, and to deal with your junk emails within your own inbox preferences.

Once the solution is deployed, you may receive emails containing specific warning banners, and emails sorted automatically into subfolders of your inbox.

Office 365 Blocked & Allowed Lists

The solution adds extra filtering security to Office 365. This solution is seamlessly integrated in Office 365, and as such, all the blocked and allowed list entries that you create on Office 365 will be applied by the filtering solution.

Example

1. You receive a message marked as spam by the solution from user@example.com.
2. Click on Report as not spam.
3. The sender user@example.com is then added directly to your Allowed Senders' list in Office 365.
4. Future messages sent by this user will no longer be blocked by the solution.

Subfolders

The filtering solution provides a way to sort messages by type, in addition to an efficient filtering.

How it works

Messages such as *social network notifications, purchase receipt, travel bookings*, etc. are individually identified by the solution.

Once identified, each message is processed depending on what your administrator has chosen, e.g. move to subfolder, delete the message, etc.

This means that additional subfolders are created automatically under your inbox to store these messages.

Example

Important: Please note that default subfolders, and the rules to move the messages in these subfolders can be customized by your administrator. As such, the examples provided below may vary depending on your corporate environment.

For example, an incoming message is identified as a *purchase confirmation.*

Your administrator chose to store this type of messages under a **Purchase** subfolder on your inbox.

You can view this message directly from this subfolder when checking your inbox.

Default subfolders

The subfolders used by default are:

Junk Folder

Contains spam and potentially harmful messages.

Newsletters

Contains newsletters you have subscribed to.

Social

Contains notifications originated from social networks.

Purchase

Contains purchase order, online payments, etc.

Travel

Contains messages related to travel arrangements, such as car rental, flight information, hotel bookings, etc.

Protecting Web links

The solution automatically protects you from phishing sites by analyzing the links contained in the messages you receive.

How it works

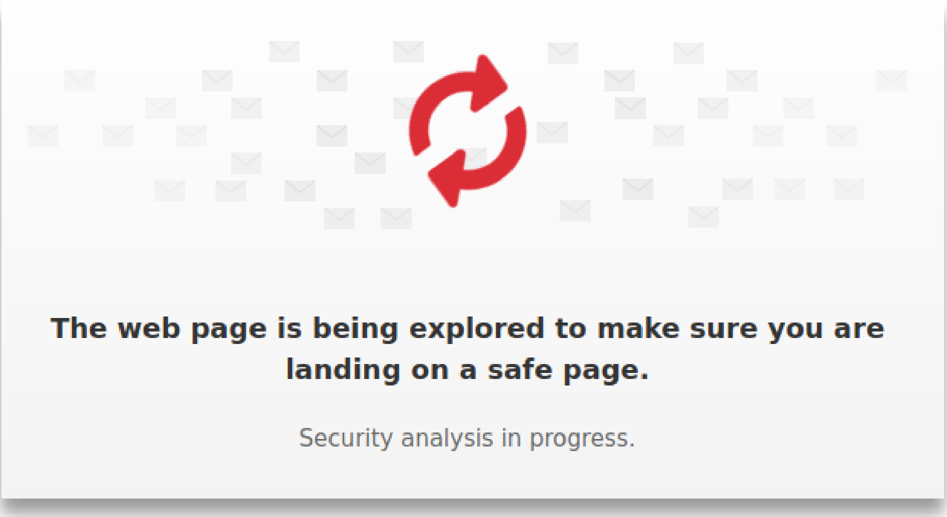
1. Upon receiving a message, the links contained in the message are rewritten to point to an analysis service.
2. The message is then delivered in your mailbox, with the rewritten links.
3. When you read the message and click on a link, the service analyzes the target website.
    - **Note**: A loading page may display for a few seconds, depending on how long it takes to analyze the target site.
4. Depending on the analysis result, the screens below may be displayed.

Pages examples

Tip: Please note that if the target website is safe, you will be redirected automatically to this site.

Loading screen

If the website analysis takes some time to complete, the following loading page will be displayed:

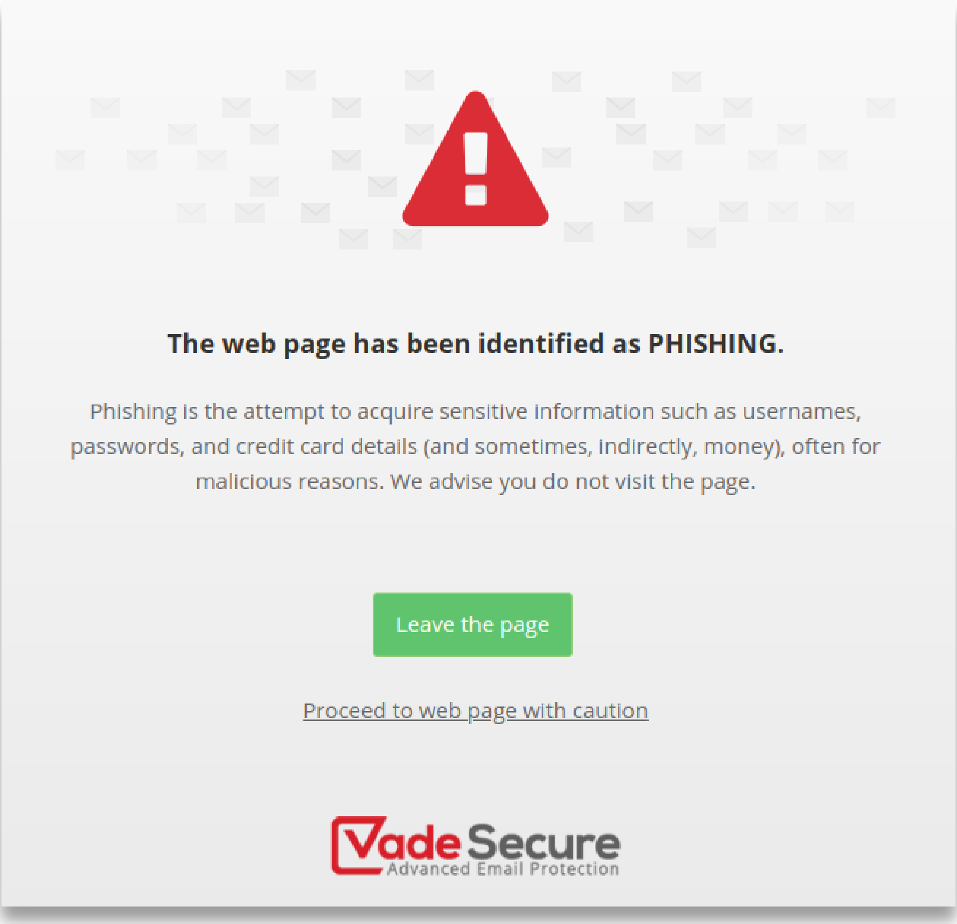


The web page is being explored to make sure you are landing on a safe page.

Security analysis in progress.

Phishing alert screen

If the website analysis unveils a malicious site, or if the link points directly to a known phishing site, your browser will display the following warning:



The web page has been identified as PHISHING.

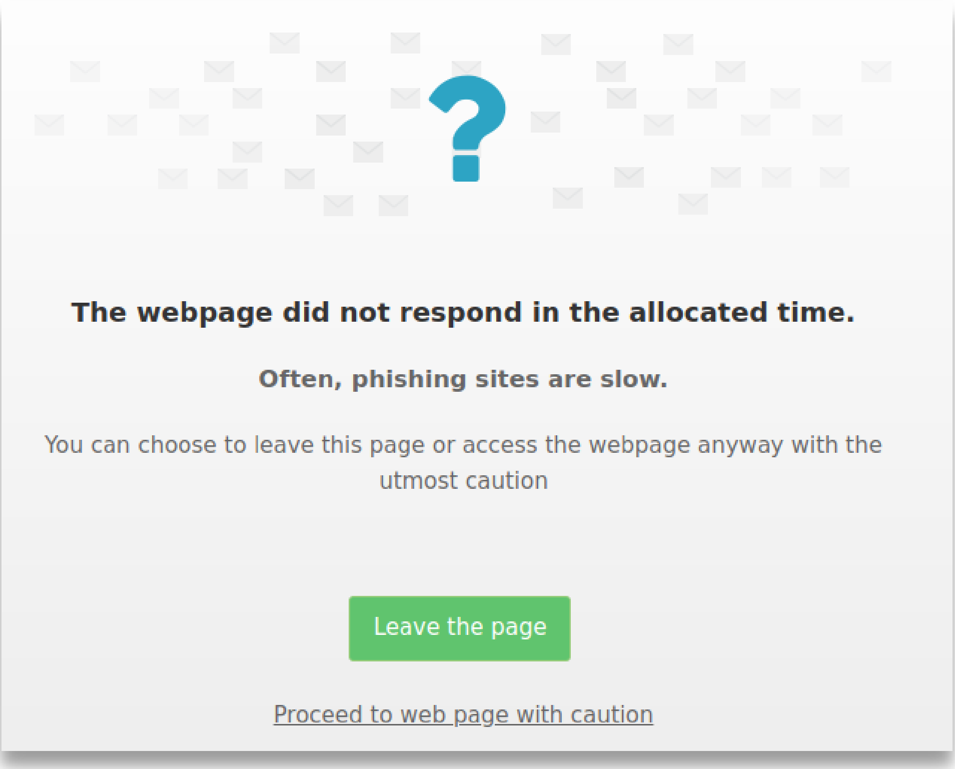
Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons. We advise you do not visit the page.

You should click on **Leave the page** to safely navigate away from the target site.

Warning! Please note that if you click on *Proceed to web page with caution* despite the warning, your administrator will receive a notification warning him you visited a malicious site.

Timeout screen

If the analysis did not complete in time, the following screen is displayed:



The webpage did not respond in the allocated time.

Often, phishing sites are slow.

You can choose to leave this page or access the webpage anyway with the utmost caution

Protecting against Targeted Attacks

The solution protects you against spoofing and targeted attacks you may receive. These attacks are also referred to as *Spear Phishing* attacks or *Fake President fraud*.

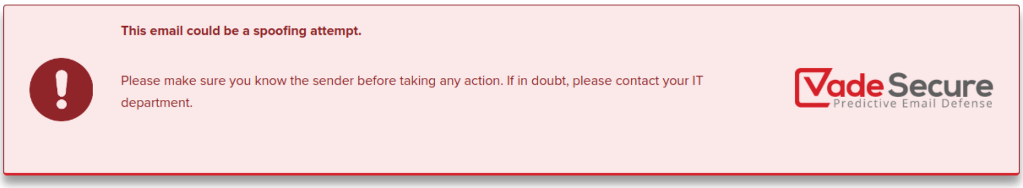
How it works

1. Upon receiving a message, the solution analyzes it to detect any potential spoofing attempt.
2. If the solution does not detect any threat, you will receive the message as is in your inbox.
3. If the solution detects a potential threat, a Warning banner is added to the top of the message to warn you about the potential threat, as displayed below.

For example, a message sent by john.doe@domainee.com or john.doe@yahoo.com, where *John Doe* is your company's CEO, and your company uses the domaine.com domain will be identified as a spoofing attempt.

Warning! Please note that these banners warn you about a **potential** risk: As such, a few legitimate messages may contain this warning banner. As a user of a corporate network, it is also your responsibility to ensure who you are replying to, and to pay attention to this kind of targeted attacks.

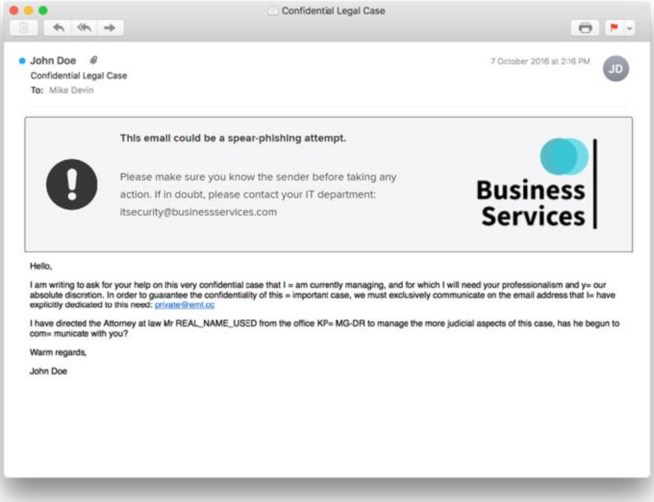
Banner examples



This email could be a spoofing attempt.

Please make sure you know the sender before taking any action. If in doubt, please contact your IT department.

Please note that the banner may vary, as your administrator can customize it:



Confidential Legal Case

John Doe
Confidential Legal Case
To: Mike Devin

7 October 2016 at 2:16 PM

This email could be a spear-phishing attempt.

Please make sure you know the sender before taking any action. If in doubt, please contact your IT department: itsecurity@businessservices.com

Hello,

I am writing to ask for your help on this very confidential case that I = am currently managing, and for which I will need your professionalism and y= our absolute discretion. In order to guarantee the confidentiality of this = important case, we must exclusively communicate on the email address that I= have explicitly dedicated to this need: private@eml.cc

I have directed the Attorney at law Mr REAL_NAME_USED from the office KP= MG-DR to manage the more judicial aspects of this case, has he begun to com= municate with you?

Warm regards,

John Doe

Protecting against Malware

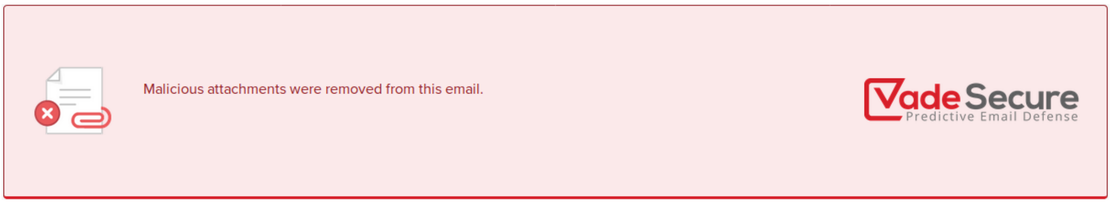
The solution protects you by analyzing the origin, the content and the context of each email.

How it works

After detecting a threat, the solution processes each message depending on what your administrator has chosen:

- **No action** (you receive the message in their inbox),
- **Delete** (the solution deletes the message),
- **Move** (the solution moves the message to another folder),
- **Remove attachments** (the solution removes the malicious attachments).

Banner example



Malicious attachments were removed from this email.