Phishing Protection - User Guide

This phishing protection solution is a critical element of protecting the organization from cybersecurity threats, such as phishing, ransomware, malware attacks, BEC attacks and much more. This guide will give you a clear overview how the solution will work, and all that you need to know.

Dynamic Banners

This solution will detect potential phishing threats and display various warning banners. It's essential to familiarize yourself with the meaning of each banner to effectively recognize and respond to threats.

System-Detected Threat

WARNING Spam, malware or phishing has been detected. Our AI is always learning, report feedback with the TitanHQ Outlook Add-In. Powered by TitanHQ™.

A warning banner is applied to an email if spam, malware, or phishing has been automatically detected.

You should be very cautious with any email which has received this banner and do not open attachments, click links, or share information unless you have verified this email has been incorrectly bannered, please see note on false positives.

Phishing Email Identified by Administrator Banner

WARNING Spam, malware or phishing has been detected. Our AI is always learning, report feedback with the TitanHQ Outlook Add-In. Powered by TitanHQ™.

This banner will appear at the top of emails which your system administrator has manually marked as phishing. You should not interact with links or attachments in emails with this banner.

Admin-Remediated Threat

WARNING Spam, malware or phishing has been detected. Our AI is always learning, report feedback with the TitanHQ Outlook Add-In. Powered by TitanHQ™.

A warning banner is applied to an email an administrator has manually remediated.

No Threat Detected

SAFE Your Administrator has marked this email as clean. Powered by TitanHQ™.

If an email is considered clean and no threat has been detected, a safe banner is applied.

Phishing Protection - User Guide

Exploited Domains

ALERT Our analysis shows that this is a suspicious domain as it is frequently used in phishing attacks. Be careful with this email. Powered by TitanHQ™.

If Exploited Domains is enabled, an alert banner is added to emails from domains known to be frequently used in phishing attacks. This is a reminder to stay vigilant, even if the content of an email does not look suspicious.

Anti-spoof

ALERT Display name spoofing has been detected. Be careful with this email unless you know it is safe. Powered by TitanHQ™.

When Anti-spoof is enabled, manipulated display names are checked, and if detected, an alert banner is added. This is a reminder to users to stay vigilant, even if the content of an email does not look suspicious. Anti-spoof default setting is disabled. Banner is applied to anti-spoof mails regardless of whether manual or auto remediation is enabled.

Graymail / Marketing Mail

INFO Our analysis indicates this is graymail (legitimate, opted-in, bulk mail). Be careful with this email unless you know it is safe. Powered by TitanHQ™.

If Graymail is enabled, it is treated as malicious, and an information banner is added to alert customers and users. This mail is moved to the user's Junk folder.

Banner is applied to graymail regardless of whether manual or auto remediation is enabled.

This mail is moved to the user's Junk folder

Using the Outlook Plugin

The THQ Outlook plug-in enables you to report phishing emails and report safe emails.

Phishing Protection - User Guide

What is a False Positive?

A False Positive is an email which you know is clean that has a PhishTitan banner. This can be reported as “Clean mail” using the THQ for Outlook add-in

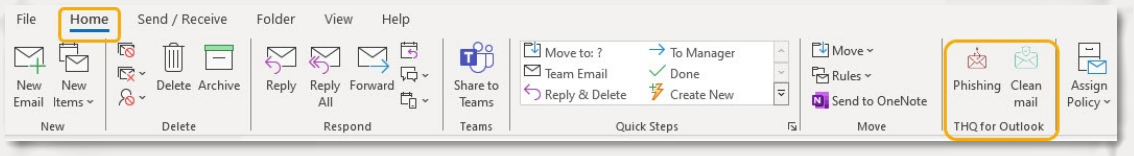
What is a False Negative?

A False Negative is an email which you suspect to be phishing that does not have a PhishTitan banner. This can be reported as “Phishing” using the THQ for Outlook add-in.

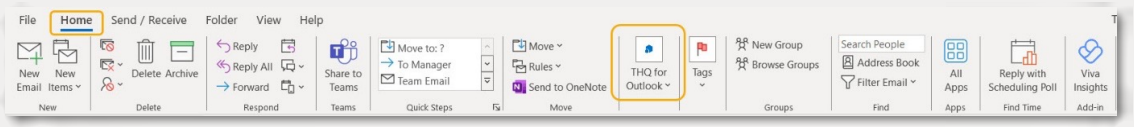
Steps to take if you identify a phishing mail.

If Exploited Domains is enabled, an alert banner is added to emails from domains known to be frequently used in phishing attacks. This is a reminder to stay vigilant, even if the content of an email does not look suspicious.

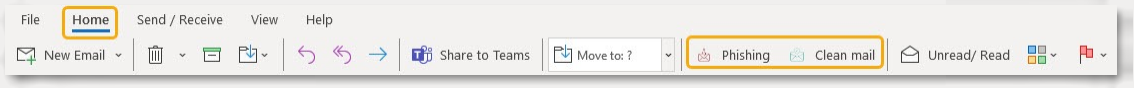
1. Classic Ribbon



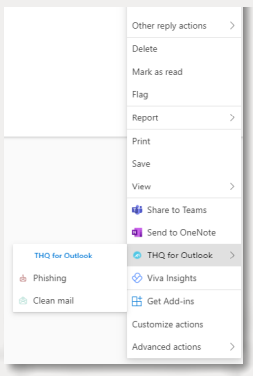
Or



2. Simplified Ribbon



3. Outlook Web Application



4. Outlook Mobile Application