

Vlad Mazek

From: Melodie Duperval
Sent: Tuesday, June 11, 2019 12:21 PM
To: Vlad Mazek
Subject: ExchangeDefender Phishing Firewall Notice

This message is sent to you by our email security service provider. If you have any questions about this feature or if there is any way we can assist you with this issue, please contact us at (555) 555-5555.

Sincerely,
Bubba's BT&Computers

ExchangeDefender is proud to announce the launch of ExchangeDefender Phishing Firewall, a service that will start protecting you from email forgery and malware. Your organization already uses ExchangeDefender to protect your email from SPAM, viruses, malware, phishing, DDoS attacks, and more. We're sending you this email to notify you of the upcoming service change that will better protect you from spear phishing: where hackers send you forged email messages in order to trick you into clicking on a link that will get you compromised. Over 90% of security breaches start with a spear phishing email and ExchangeDefender Phishing Firewall will help protect you by notifying you when you click on a link that is potentially dangerous. The process is designed to secure you transparently, but if you click on something potentially dangerous you will see the following screen:



ExchangeDefender does not have a security profile for this URL, please click only if you recognize the site at your own risk:

Link: <https://support.ownwebnow.com/task-list.php?task=ad61ab143223efbc24c7d2583be69251>

Whitelist this web site

Blacklist / Ban this web site

Sender Domain: harambe.exchangedefender.com

Link Domain: support.ownwebnow.com

Is it likely that someone from harambe.exchangedefender.com would be sending you a link at support.ownwebnow.com?

From: root@harambe.exchangedefender.com

To: joel@ownwebnow.com

Message ID: x55jt2Qe014752

Why am I seeing this?

ExchangeDefender Phishing Filter has been enabled to provide additional security for your domain ownwebnow.com and reduce the risk of spear phishing. Hackers often employ fraudulent practices such as sending emails seemingly from a known or trusted sender. Their hope is that you will click on the link and go to their web site where they can either infect your computer or try to get you to reveal confidential information such as your password or other information useful in identity theft.

ExchangeDefender intercepts web site links in your email messages and automatically rewrites them so they must pass through this web site. If the site is on a whitelist and is trusted, you will be automatically redirected. If the site is unknown or dangerous, ExchangeDefender will display this warning page to alert you about possible security issues.

This screen will be displayed when you click on a link in your email that has not been marked as safe by your IT administrator or IT Solution Provider, and that is not listed in our database of web sites with good reputation. You will see the link you clicked, critical tracking information about the email it was in, sender information, recipient information, etc. If you recognize the sender and are expecting the message, clicking on it will automatically redirect you there.

If you are signed in to ExchangeDefender admin portal, you will also see two buttons: Whitelist this web site and Blacklist / Ban this web site. If you whitelist the web site, you will not be shown this alert screen again in future when clicking on email links to that web site.

For more information and security best practices, please take a look at the ExchangeDefender Phishing Firewall User Guide:

<https://www.ExchangeDefender.com/media/ExchangeDefenderPhishingFirewallUserGuide.pdf>

This service will automatically start protecting all ExchangeDefender Pro users starting on Thursday, June 13, 2019 at 5 PM EST (21:00 GMT).

This is a one-off email from For more information, please contact your IT service provider:

Service Provider Logo

Service Provider Name

Service Provider Address

Service Provider Web Site