

The Answer to Phishing Links in Microsoft Office 365

Office 365 continues to use a detect-and-respond approach to cybersecurity. Menlo Security's Internet Isolation Gateway can make sure your users are safe from phishing attacks.

Benefits:

- Prevent malware from being delivered to users' devices through phishing links in email
- Render suspicious web forms as read only to prevent users from entering their credentials into fake login pages
- Integrate directly into Office 365 platform and workflows
- Maintain native email and web-browsing experience
- Gain powerful insights into phishing attempts and users posing the most risk to the organization
- Customize time-of-click messages that enhance anti-phishing education

Office 365 Is a Tempting Target

Microsoft Office 365 is one of the fastest-growing cloud applications ever, with more than 135 million monthly active users at the end of 2018, according to the company. And this growth makes sense. Any organization already using Word, Excel, PowerPoint, and Exchange should want to take advantage of the power, accessibility, and scale of the cloud.

However, the success of Office 365 is a blessing and a curse. Those 135 million users are also 135 million potential targets for phishing attacks. Malicious actors can easily spin up an authentic-looking email branded with a fake Microsoft logo and send it to targets, knowing that there's a good chance they are Office 365 users. From there, they can direct users to a malicious site where malware is downloaded onto their device, or they can entice users to enter their credentials into a fake web form. Once a device is infected, an attacker knows that it's fairly easy to infiltrate the corporate network and other critical business systems. According to Microsoft, 100 million malicious emails targeted Office 365 users in 2017.

Security Issues with Office 365 Email

The problem is that Office 365 uses traditional email security solutions that haven't evolved to meet today's cybersecurity demands. The two plug-ins that enterprises can add to their Office 365 subscriptions—Exchange Online Protection (EOP) and Advanced Threat Protection (ATP)—continue to rely on a detect-and-respond approach. The URL rewrite feature allows only an allow-or-block determination and operates only one click at a time. If malicious content is not detected at the time of click, users can be sent to a malicious site or a fake web form.



100 million malicious emails targeted Office 365 users in 2017.

Menlo Security Internet Isolation Gateway

Enterprises can harden their Office 365 email security posture by adding isolation capabilities on top of existing cybersecurity solutions and techniques. Menlo Security's Internet Isolation Gateway can be deployed within an existing Office 365 or Exchange Online email workflow, and it rewrites all web links a user receives in Office 365 email messages. If a user clicks on a suspicious web link in an email, the questionable website is opened within the cloud-based Menlo Security Isolation Platform (MSIP) and only safe, mirrored content is rendered on the user's local browser. In addition, policies can be set to render suspicious web forms as read only to prevent credential theft.

No Impact to Users' Email Experience

Most importantly, the Menlo Security Internet Isolation Gateway does not impact users' email experience. They can continue to use the Office 365 email client and webmail on the same browser they've always used. They can continue to click on any link in an email and access any web content they need for their day-to-day responsibilities—and know that they are safe. Nothing is changed. The only difference is a banner that sits across the top of the browser, assuring users that the web content they are viewing is being isolated in a remote browser instead of on their device.

Better Reporting and Insight

Menlo also offers better reporting and insight into malicious activity. A company's security team can see repeat offenders within the enterprise and can customize time-of-click messages to provide anti-phishing education.

How Secure Is Secure?

Many organizations feel that Microsoft's add-on detection-based security offerings for Office 365 are "good enough." But is "good enough" really enough when your use of the Office 365 platform makes you susceptible to sophisticated phishing attempts? All it takes is one successful attack, one breach. Adding Internet isolation capabilities provides comprehensive protection against phishing attacks. Isn't your organization's users, business systems, and data worth it?

To find out how Menlo Security solutions can protect your organization, contact us at ask@menlosecurity.com.

About Menlo Security

Menlo Security protects organizations from cyberattacks by seeking to eliminate the threat of malware from the web, documents, and email. Our cloud-based Isolation Platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end-user experience. Menlo Security is trusted by major global businesses, including Fortune 500 companies and financial services institutions.

© 2019 Menlo Security, All Rights Reserved.

Contact us
[menlosecurity.com](https://www.menlosecurity.com)
(650) 614-1705
ask@menlosecurity.com

