6 Ways Office 365 Keeps Your Email and Business Secure

Office

Microsoft

Introduction

We've made email security our priority, so you don't have to make it yours.

Email is the lifeblood of corporate communication and the gateway to any business, but securing it doesn't need to be a massive undertaking for your IT team. Office 365 uses the latest technologies to keep email data private and protected from ever-evolving threats—all while remaining mobile and accessible from your desktop or anywhere with an internet connection. Because these security features are all built-in and update automatically, your company's protection requires minimal involvement on your IT team's end.

Flip through to learn how Office 365 can help protect your organization's email from advanced threats.

1. Keep your data private and under your control

A cloud-based solution for email is only as good as its data privacy and service provider transparency. You need to feel confident in where the data resides, who has access, and what's being done with your broader company information.

Unlike other hosted email providers, we don't mine your data, which can potentially leak sensitive company information, and we don't share it with third parties. Your data remains yours and under your control, allowing you to determine who has access to it. We tell you where your data resides, who has access, and when.

We're always accountable to you. Whether it's providing proactive controls that you can use to maintain organizational compliance or enabling the freedom to take your data with you should you ever choose to switch providers—Office 365 is built on the core tenet that it's your data, no matter what.

87%

of surveyed IT professionals are concerned or very concerned about the privacy of cloud data, according to a Dimensional Research survey conducted for Druva.[1]

2. Manage external threats

CONTROL WHAT COMES IN

Email traffic control remains a high priority, since it's often how malware reaches your organization. As attacks become more sophisticated, your company could be vulnerable—ultimately risking the loss of intellectual property, productivity, reputation, time, and money.

Robust security features that protect against spam, viruses, and malware are beneficial for any email solution, but increasingly sophisticated attacks threaten email security despite these safeguards. For external threats, Office 365 gives you the option to use Advanced Threat Protection (ATP) to guard mailboxes against sophisticated attacks in real time. Email attachments and links are automatically evaluated for suspicious activity, and malicious content is neutralized. Zero-day protection begins the moment Office 365 Advanced Threat Protection is implemented.

97%

of people globally can't correctly identify a sophisticated phishing email, reports Intel Security.[2]

3 Benefits of Office 365 Advanced Threat Protection:

1. PROTECTION AGAINST UNKNOWN MALWARE AND VIRUSES

All messages and attachments without a known virus/malware signature are routed to a special hypervisor environment, where a behavior analysis is performed using a variety of machine learning and analysis techniques to detect malicious intent. If no suspicious activity is detected, the message is released for mailbox delivery.

2.REAL-TIME, TIME-OF-CLICK PROTECTION AGAINST MALICIOUS URLS

ATP's Safe Links feature proactively protects users who click on seemingly safe links that forward to unsafe sites—dynamically blocking malicious links when they're clicked, while permitting access to safe ones.

3. RICH REPORTING AND URL TRACE CAPABILITIES

With critical insights into who is being targeted in your organization and the category of attacks you are facing, reporting and message tracing enable you to investigate any messages blocked for unknown viruses or malware. URL trace capability lets you track individual malicious links in the messages that have been clicked.

Watch a short video on Office 365 Advanced Threat Protection: https://resources.office.com/en-us-landing-advanced-threat-protection-live-action-video.html

Be proactive

Taking a proactive approach to protecting your organization's safety, Office 365's email filtering capabilities detect and suppress external threats, while providing admins with visibility into targets and options for mitigating or eliminating attacks.

DYNAMIC DELIVERY OF SAFE ATTACHMENTS

This feature minimizes productivity delays when scanning attachments. The email recipient will receive the body of the email with a placeholder attachment, while the suspicious attachment undergoes a scan, enabling recipients to continue to read and respond to messages. If the attachment is cleared, the placeholder is replaced; if the attachment isn't cleared, the admin can filter out the unwanted (potentially malicious) attachment.

ZERO-HOUR AUTO PURGE

If a message delivered to an employee's inbox is later found to be spam, Zero-Hour Auto Purge moves it from the inbox to the spam folder. The reverse is true for messages misclassified as spam.

SAFETY TIPS FOR OUTLOOK ON THE WEB

Color-coded safety tips appear across messages indicating whether they are suspicious, unknown, trusted, or safe—alerting users to potentially fraudulent requests or other suspicious activity.

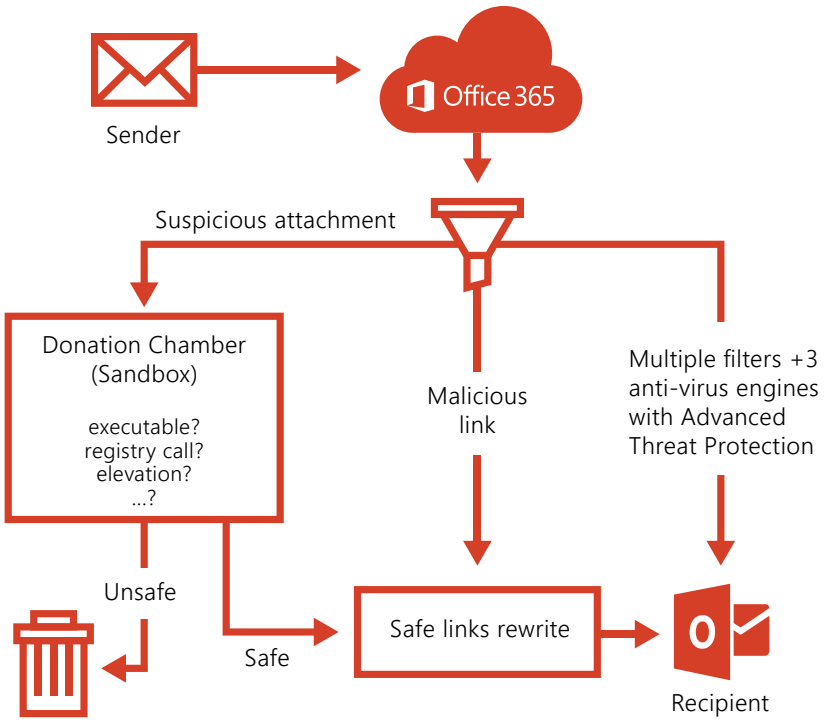
PHISH REPORTING

To better recognize phishing messages, this feature enables users to report any suspicious-looking messages as phishing—similar to reporting junk mail. These emails will be reviewed and added to the service-wide filters if they meet the classification criteria.

FILTERING COMMON MALICIOUS ATTACHMENT TYPES

Recently launched, this provides an easy-to-use tool for Exchange Online Protection admins to filter out unwanted and potentially malicious attachments by file type within the Malware Policy. This consolidates attachment filtering for malicious content, rather than addressing these issues through transport rules and malware filtering policies.

SECURE YOUR MAILBOX AGAINST ADVANCED THREATS



Protect your inbox

Office 365 comes with a junk email filter to keep unwanted messages out. You can also help prevent junk emails from slipping through and keep good emails from heading to the spam folder with customizable settings to fit your organization's needs.

SAFE SENDERS LIST

Automatically considered safe, email addresses and domain names in the Safe Senders List are never treated as junk email, regardless of the content of the message.

SAFE RECIPIENTS LIST

Messages sent to these email addresses or domain names are never treated as junk, regardless of the content of the message.

BLOCKED SENDERS LIST

Messages from people or domain names that appear in this list are always classified as junk, regardless of the content of the message.

BLOCKED TOP-LEVEL DOMAINS LIST

Add country/region codes to block unwanted email messages from another country/region. For example, checking the CA (Canada), US (United States), and MX (Mexico) boxes in the list blocks messages from any email addresses that end in .ca, .us, and .mx.

BLOCKED ENCODINGS LIST

To block unwanted email messages that appear in another character set or alphabet, add encodings to the Blocked Encodings List.

3. Step up security to fight internal threats

You need to know that company emails are protected however or wherever employees work. Security threats come from all sides—including internally. With a solution that defends against attacks and proactively prevents data loss, you can protect your business on both fronts.

Only 23% of respondents in a CyberEdge Group defense report are confident their organizations have made adequate investments to monitor privileged users' activities.[3]

Despite malicious malware and viruses, user error is often a cause of data loss. To protect information internally, administrators can control email access permissions using information rights management (IRM) to keep unauthorized people from printing, forwarding, or copying sensitive information. Users can apply IRM policies to a specific email or create rules that automatically apply to emails that meet specific criteria.

Your management of transport rules, actions, and exceptions can give your team the control they need without affecting mail flow.

Data Loss Prevention (DLP) can proactively scan emails and notify users before they send sensitive information, like social security or credit card numbers. Not only will this help prevent sensitive information from leaking, but with the help of DLP Policy Tips you can educate your employees on best practices and minimize security risks in the future.

As employees use Office 365 through Outlook on the web, enterprise-level authentication and security certification help to enhance data security. We know how important it is for your team to have your software and data available to you when you need it, while still prioritizing email security.

4. Secured email access from mobile devices

The workforce has become more mobile than ever with the rise of smartphones and tablets, giving employees the freedom to work from internet-accessible locations whenever they want. Increased use of personal devices has created a bring-your-own-device (BYOD) culture and has empowered employees to work on the go.

But this mobile freedom comes at the risk of potentially compromising important business data. Together, Outlook 2016 and Exchange Online protect your email data—no matter where your users are connecting.

With mobile device management (MDM), you can manage access to Office 365 data across a range of phones and tablets, including iOS, Android, and Windows Phone devices.

Control the information accessible from mobile devices by setting up policies for accessing Office 365 resources. Block access on phones and tablets that fail to meet security and encryption standards in order to prevent unauthorized access to your company's information.

Allow for mobility without increasing security risks. If a device gets lost or stolen or an employee leaves the company, security features help prevent unauthorized user access. You can remove Office 365 company data from their personal device, while still leaving their own data in place.

56%

of enterprises surveyed by EY admit to being unlikely to detect a sophisticated mobile threat.[4]

5. Stay compliant, simply

Constantly shifting regulatory and industry standards can make it difficult for IT teams to maintain compliance, let alone take a proactive approach. Helping to alleviate these pain points, Microsoft is a trusted partner in adhering to compliance standards across multiple industries.

With Office 365, you're no longer reliant on stitching various compliance solutions together. Your company email and all Office 365 applications automatically adhere to 10 rigorous privacy compliance standards across a variety of industries, including medical (HIPAA), government and homeland security (DPAS & FISMA), education (FERPA), and banking. With more than 900 controls in the Office 365 compliance framework, all Office 365 applications stay up to date with ever-evolving privacy compliance standards.

In the event of an information request or compliance issue, Office 365 makes it simple to quickly find, analyze, and package the relevant electronic content with eDiscovery. The Office 365 Security and Compliance Center's privacy controls let you instantly grant access to whomever needs to gather the information. Use the eDiscovery Administrator role to enable team members to perform searches and place holds on mailboxes, SharePoint Online sites, and OneDrive for Business locations. Members can also create and manage eDiscovery cases, add and remove members on a case, and create and edit content searches. Managing these tasks from one location can lessen the burden on your IT team, helping free up their time and enabling them to tackle more important initiatives.

6. Remain confident with continuous updates

Security and compliance issues are forever changing, making it difficult for your IT team to keep security measures up to date. Maintaining the latest versions of essential applications is the best way to combat increasingly sophisticated security threats. But by utilizing Office 365's automatic updates, your IT team can focus on more important projects. You can also opt for manual updates to keep control within your IT team.

Office 365 keeps upgrades and patches current in a predictable manner across all registered devices. With 99.9% financially backed uptime, you can count on your company email to stay up and running.

Ready to secure your organization? Take a guided tour to learn more about Office 365.

Sources

[1] "The State of Data Privacy in 2015," 2015, Druva and Dimensional Research

[2] "Intel Security Phishing Quiz Results," 2015, Intel Security

[3] "2015 Cyberthreat Defense Report North America & Europe," 2015, CyberEdge Group

[4] "Get Ahead of Cybercrime: EY's Global Information Security Survey 2014," EY

Office

Microsoft