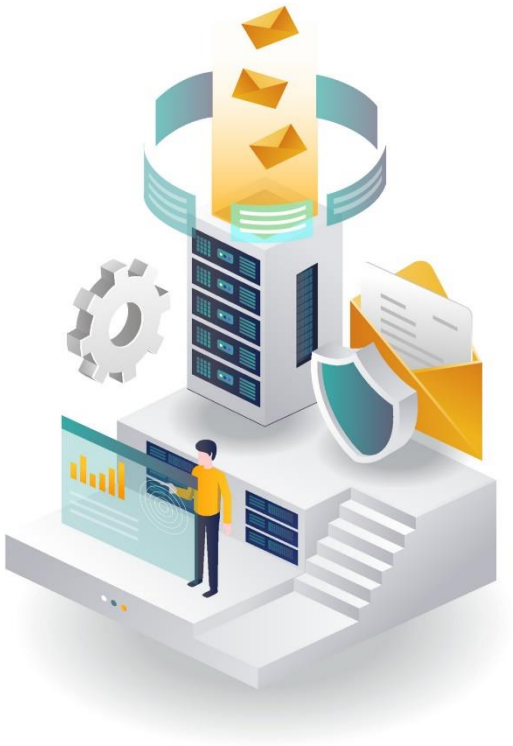
Close Gaps in Microsoft 365 Outbound Email Protection with SendGuard for Outlook

Protect your company from the risk of confidential information being emailed to the wrong recipient.



Microsoft offers a range of security features to protect outbound emails within their ecosystem. Many organizations question whether the built-in email security of Exchange Online Protection or Microsoft Purview DLP offers sufficient safeguards to protect their users, data, and communication against outbound email security threats.

The level of protection may differ based on the licensing of each user, and while Microsoft consistently enhances its email security features, there are still some vulnerabilities that exist.

1. Risk of emailing the Wrong Recipient

According to a report by the UK Information Commissioner's Office **data emailed to the wrong recipient is one of the leading data breaches reported.**

Inadvertent human errors can lead your employees to send sensitive emails or files to unintended recipients.

sales@standss.com

Gap in Security

MailTips is a feature in Exchange Online that provides users with real-time information about the message they are composing.

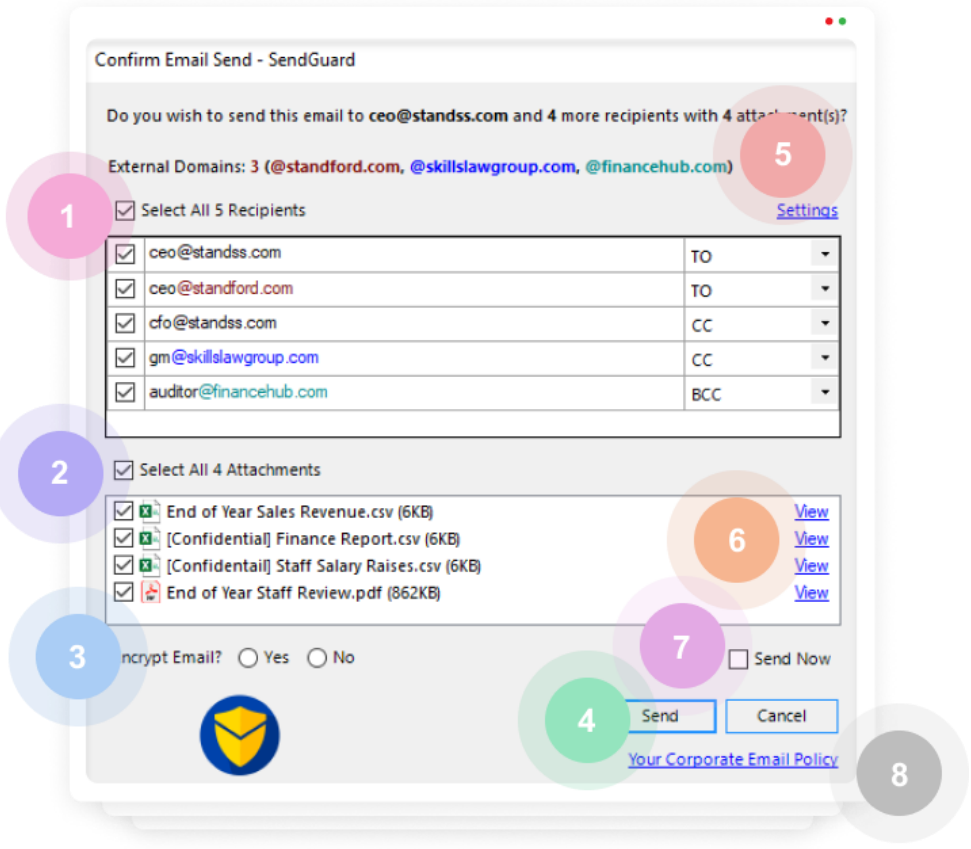
However, Mail Tips does not provide any protection from emailing the wrong recipients. It does not allow users to prompt recipients and attachments in outgoing emails.

For organizations that handle confidential data, it is very important to secure their email communications, especially when they send emails to external domains (i.e. outside their own organization).

Article 5 of GDPR states that **Information must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.**

How can SendGuard help

SendGuard stops accidental data loss from **misaddressed emails** or **incorrectly attached files** before they happen by prompting users to **confirm recipients and attachments in outgoing emails**.



1. Review **Recipients**
2. Review **Attachments**
3. (Optional) **Encrypt** the email
4. Click Send (SendConfirm can even **log details** of email sent)
5. **Color-coded External Domains** for easy Identification
6. **View Attachment**
7. Sent Now or Delay (to allow **Unsend/Recall**)
8. Brand with your logo, **Customized wording and links** to email policies

sales@standss.com

Even organizations using the most advanced protection available in Microsoft 365 will benefit from implementing SendGuard as Microsoft Purview does not allow to confirm recipients and attachments.

SendGuard acts as a nice check and balance tool on your typically fast-paced email input.

2. Inability to perform Customized Security checks on Outbound Emails

Different organizations have unique security requirements based on their industry, size, compliance needs, and risk profile.

You may need certain email checks to be carried out on emails before sending them out, such as **preventing groups from emailing each other**, requiring **confirmation before emailing large groups**, and **automatically encrypting emails.**

Customization allows security to be adjusted to fit the specific needs of an organization, providing more targeted protection.

Gap in Security

Performing specialized security checks on emails is only **possible with the more expensive Microsoft plans** and add-ons that include Microsoft Purview. Additionally, these checks are conducted on the server-side, **which may result in a delay before senders are notified.**

How SendGuard can help

The SendRules component of SendGuard allows you to **specify your own rules that will be run on outgoing emails.**

SendRules uses the **IF THEN model** to create rules that alert the user if they send a message that has matched a rule. You can configure the rules to match all the conditions in the rule or stop on the first rule.

Examples of rules you can create are:

- If the recipient contains one or more email addresses from the "finance team"
- If the recipient contains ANY email addresses excluding "@standss.com"
- If sending to the following distribution lists/contact group "test@standss.com"
- If sent from the email address/domains "gmail.com"
- If email/attachment has text "Credit Card"
- If sending to multiple domains excluding "standss.com"
- If email has sensitive information (you can create your sensitive information type or choose from available templates)

- If attachment exceeds a certain size

You can THEN:

- Display a customized prompt warning with Yes/No buttons, warning with OK/Cancel, or block the message altogether.
- You can automatically add recipients in the CC or BCC field for compliance, legal, or specific business requirements.
- You can append additional text to the subject.

Standss can create custom scripts for your organization for advanced checks.

We can help you create custom rules to identify and block outgoing emails that contain intellectual property, trade secrets, or proprietary information, customer PII unique to your business and enforce business communication standards (formatting, branding, and requiring disclaimers).

3. Emailing Sensitive or Inappropriate Content (Email Data Loss Prevention)

An email DLP solution can help prevent data breaches, data leakage, and accidental data loss caused by insider threats or human errors, such as sending an email to the wrong recipient or attaching the wrong file.

Microsoft allows you to create data loss prevention policies (DLP) that include **policy tip notification messages, email notifications** and **oversharing pop-ups** to prevent email users from inappropriately sharing sensitive information.

Gap in Security

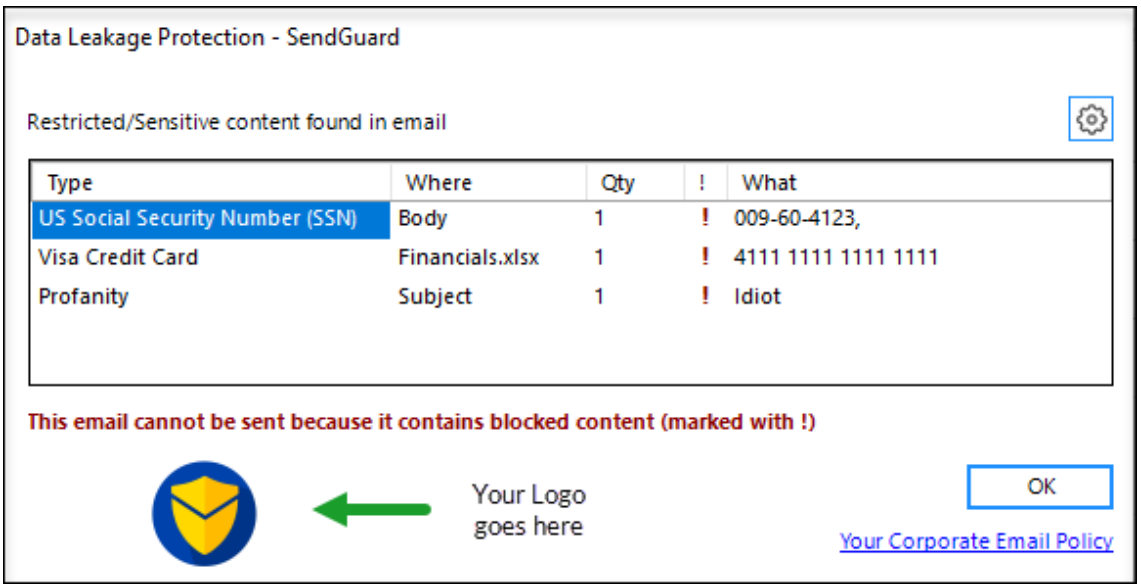
DLP is a premium feature that is available on plans like Business Premium, Microsoft/Office 365 E3 and Microsoft/Office 365 E5 subscription. Microsoft Purview DLP for emails and files is not accessible for users on plans like Microsoft 365 Business Basic/ Standard and Microsoft/Office 365 E1.

This leaves your organization vulnerable to data loss via email.

How SendGuard can help

IT admins can configure SendGuard DLP to scan emails for Credit Cards, Social Security Number, Profanity Lists, and any other sensitive data.

SendGuard can **scan email content** (body, subject and attachments) for specific words or data patterns and warn/block users if it finds any potentially sensitive or restricted content.



Email users receive **real-time prompts** when they have violated any of the DLP policies that are created.

4. No Reply-All Protection

Using “reply-all” in email communication can cause problems when it is not used properly or too frequently. It can result in too many emails, wasted time, confusion, and **the accidental exposure of sensitive information.**

These problems can get worse when there are large distribution lists or too many replies to company-wide emails.

Gap in Security

Microsoft offers no protection against “reply-all” and there is no way to prevent accidental data exposure caused by users emailing unintended recipients.

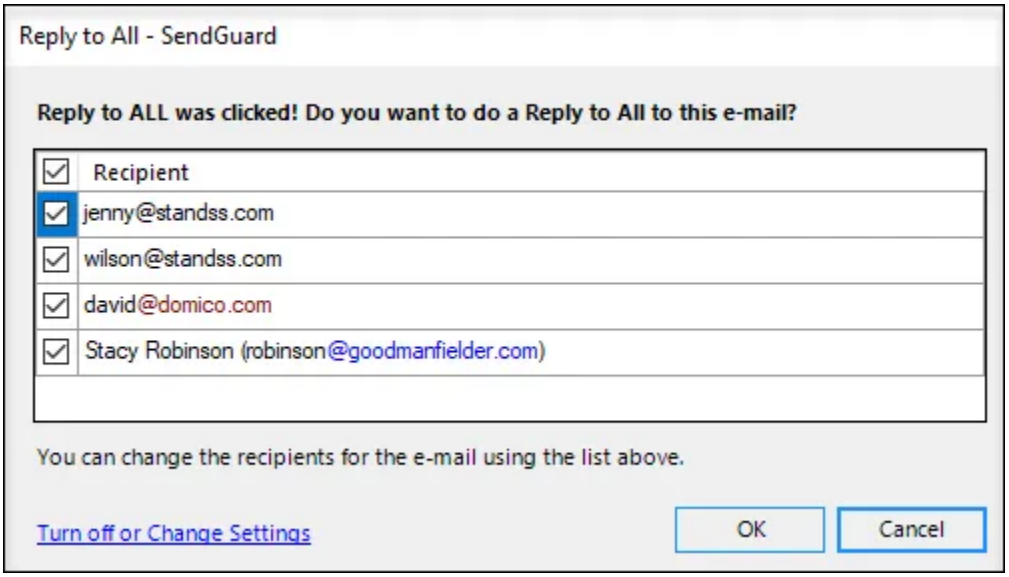
How can SendGuard help

The **ReplyGuard** feature of SendGuard **encourages off email resolution** by prompting users to use chat/phone call if their replies have exceeded the limit set by your organizational email policy.

sales@standss.com



ReplyGuard also gets email users to view and confirm recipients any time they click Reply or Reply-to-All on an email with multiple recipients.



External domains are color-coded for easy identification.

If you are using a distribution list, you can also view the members of the distribution list as well before sending your email.

sales@standss.com

5. Unsend emails even after clicking Send

People may want to unsend an email for various reasons, such as correcting errors or typos in an email that has just been sent.

It's also common to accidentally send an email to the **wrong recipient containing sensitive/confidential information** that should not have been shared with that individual. In some cases, emails are sent impulsively, and the sender later realizes it was a hasty decision.

Additionally, regrettable content in an email can lead to a desire to retract it to avoid potential conflicts or misunderstandings. **Legal or ethical concerns** may also prompt the need to unsend an email, particularly if the email contains problematic information. **Privacy** is another significant consideration; individuals might wish to retract an email that contains personal or sensitive details.

Gap in Security

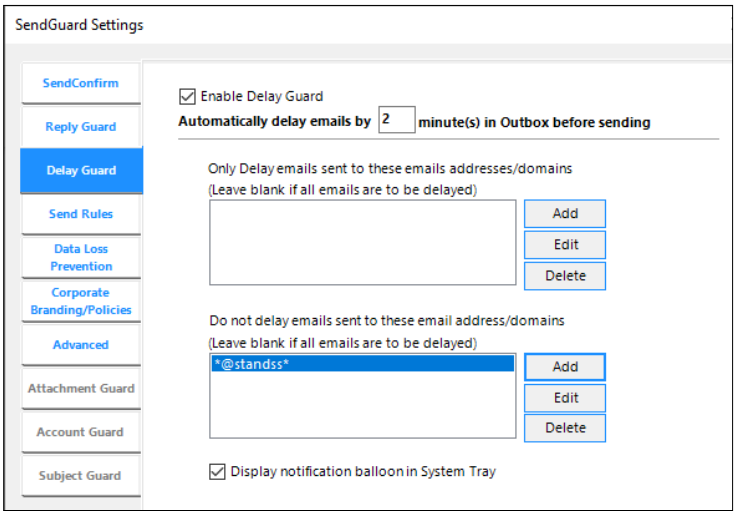
Recalling an email is **not always reliable** and depends on the recipient's email system and settings. If the recipient has already opened and read the email, the recall will likely be ineffective.

Email **recall is time-sensitive**, and if you realize your mistake too late, the recipient may have already read the email and acted upon it. In addition, the email may not be recalled from all the devices the recipient accesses their email account from.

In such cases, delaying emails can serve as a safety net. It gives you a brief window to retract the message or make necessary corrections before it reaches the recipient's inbox. However, delaying emails in Microsoft Outlook is challenging and **cannot be easily implemented at an organizational level**.

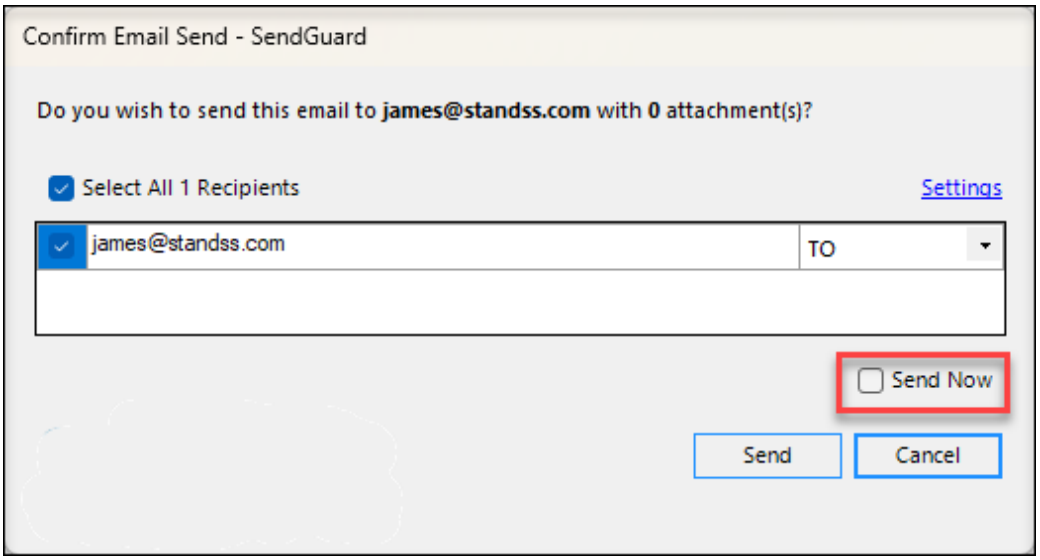
How can SendGuard help

The DelayGuard component in SendGuard can delay all emails or only **those sent to specific email addresses and domains.**



sales@standss.com

For urgent emails you can select the **Send Now** option on the SendConfirm prompt to bypass the delay delivery.



Note: Administrators can choose to hide the **Send Now** checkbox for users.

Request a Personalized Demo

To see a full range of features and benefits, customizations, and volume pricing quotes, contact us on sales@standss.com for a tailor-made demo.

Overcome native Microsoft 365 outbound email security limitations by using SendGuard Email Protection.