Information Security, Risk & Compliance

10 Ways to Protect Users from Emailing Sensitive Information to the Wrong People

10 Real World Scenarios

Introduction

The need to pay attention to **Risk and Compliance related to outgoing emails** is increasing as we see a rise in **international, national, and industry-specific data privacy regulations.**

The risk is compounded by the fact that it is too easy (Outlook Auto-Complete, Reply-All etc) to accidentally send emails and attachments to the unintended recipients.

Costs can be high for organizations that do not take adequate steps to prevent this data leakage. These costs can range from loss of reputation to the loss of income and clients, to lawsuits and even penalties and fines based on GDPR and other data security/protection legislation.

SendGuard is an Outlook add-in that has a number of "guards" **to check emails and warn users of potential problems before emails are sent out**.

In this white paper, we showcase 10 use cases of how clients are using SendGuard for Outlook **to protect users and organizations from sensitive information being emailed to unintended recipients**.

Use cases highlighted include:

1. Prompt users to confirm Recipients and Attachments before emails are sent out
2. Reduce the use of Reply-All
3. Block emails or attachments with certain words (e.g. profanities)
4. Warn users if email contains potentially sensitive or confidential information
5. Delay (External) Emails to allow Unsend
6. Prevent emails from being sent to conflicting recipients
7. Include Attachments with Replies
8. Encrypt Outgoing emails using Existing Server Software
9. Build Chinese Walls – Prevent groups of users from emailing each other
10. Use the correct Outlook (sender) account to send emails

[Bonus Feature] Mass Marketing Risk Compliance

We hope that these use-cases will spark ideas of new ways to protect your users. If you have a use-case that is not covered in this list, please let us know (sales@standss.com). Our team is available to help configure and if necessary, upgrade SendGuard to fully meet your email security requirements.

1. Prompt users to confirm Recipients and Attachments before emails are sent out

Goal:

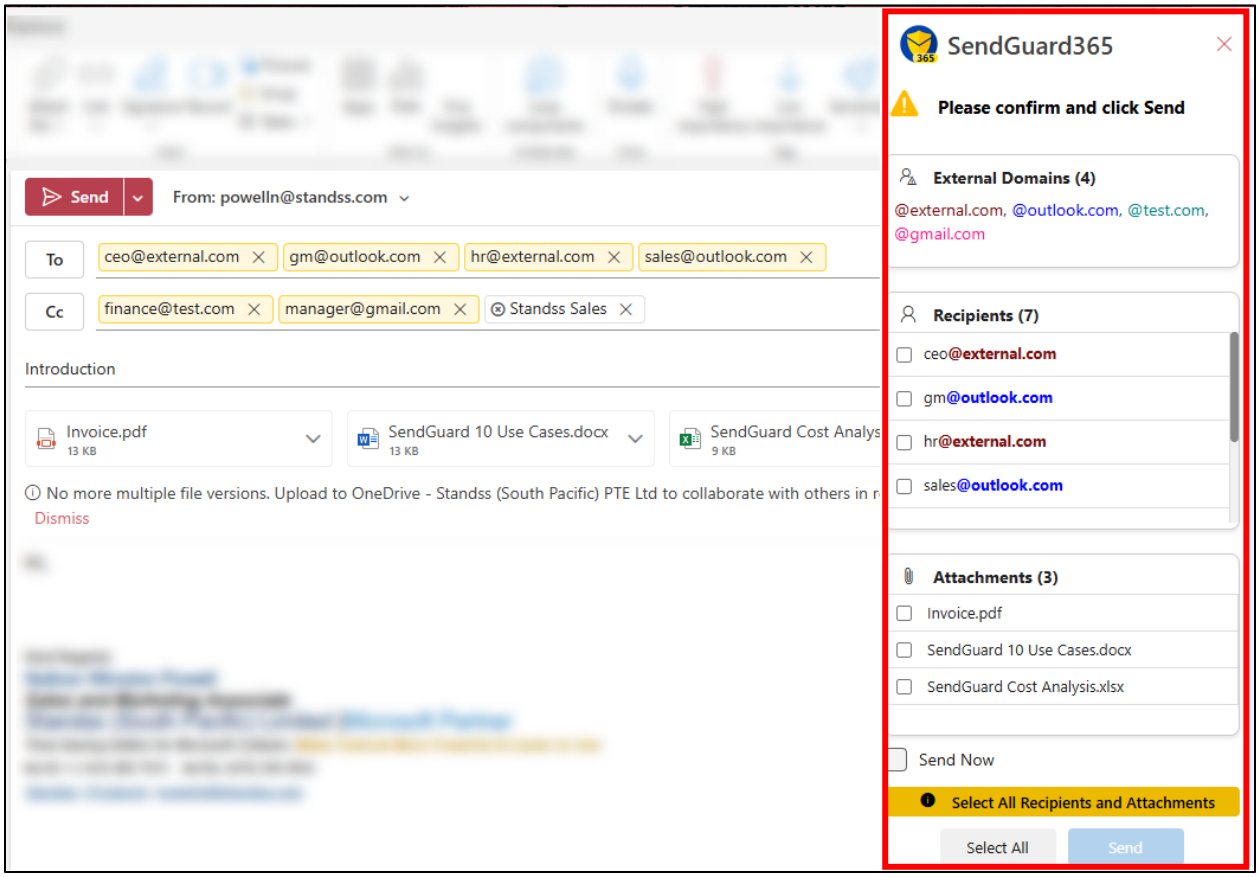
Force users to review and confirm recipients and attachments before emails are sent out.

Clearly identify external recipients that the email will be sent to.

(Optional) Protect the organization by keeping a log of emails that users have chosen to send.

Solution:

The **SendConfirm component of SendGuard** prompts users with a list of recipients and attachments before an email is sent out. **Users can see (and change) who the email is going to**.



Users can also **open attachments directly** from the same screen.

The prompt also **color-codes recipients to highlight the different external domains** the emails are being sent to.

Finally, administrators can configure SendGuard **to keep a log of basic details of emails** that were confirmed by the user for sending.

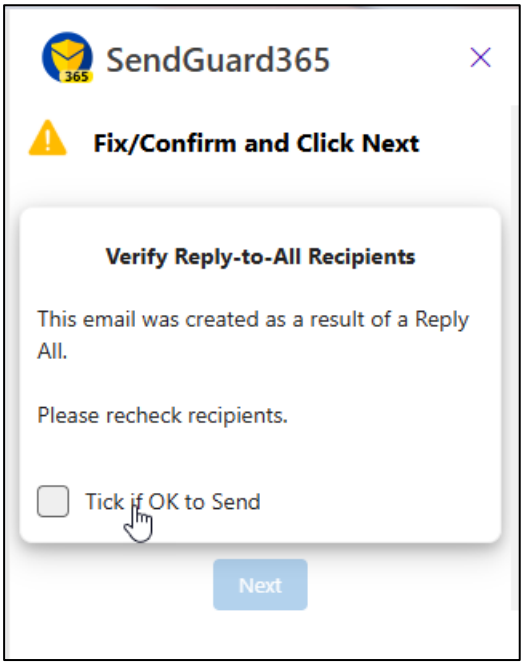
2. Reduce the use of “Reply-All”

Goal:

Reduce the indiscriminate use and resulting “internal spam” and wasted time caused by unnecessary “Reply-All’s”. Ensure users are aware of exactly who they are sending the email to when they click “Reply-All”. Give users the ability to disable the Reply-All button on (internal) emails they send out.

Solution:

(For received emails with multiple recipients) The **ReplyGuard component of SendGuard** prompts for **confirmation** anytime the user clicks “Reply-All”. The prompt can be a simple message, or it can **show exactly to whom the email is going to**.



3.Block emails or attachments with certain words (e.g. profanities)

Goal:

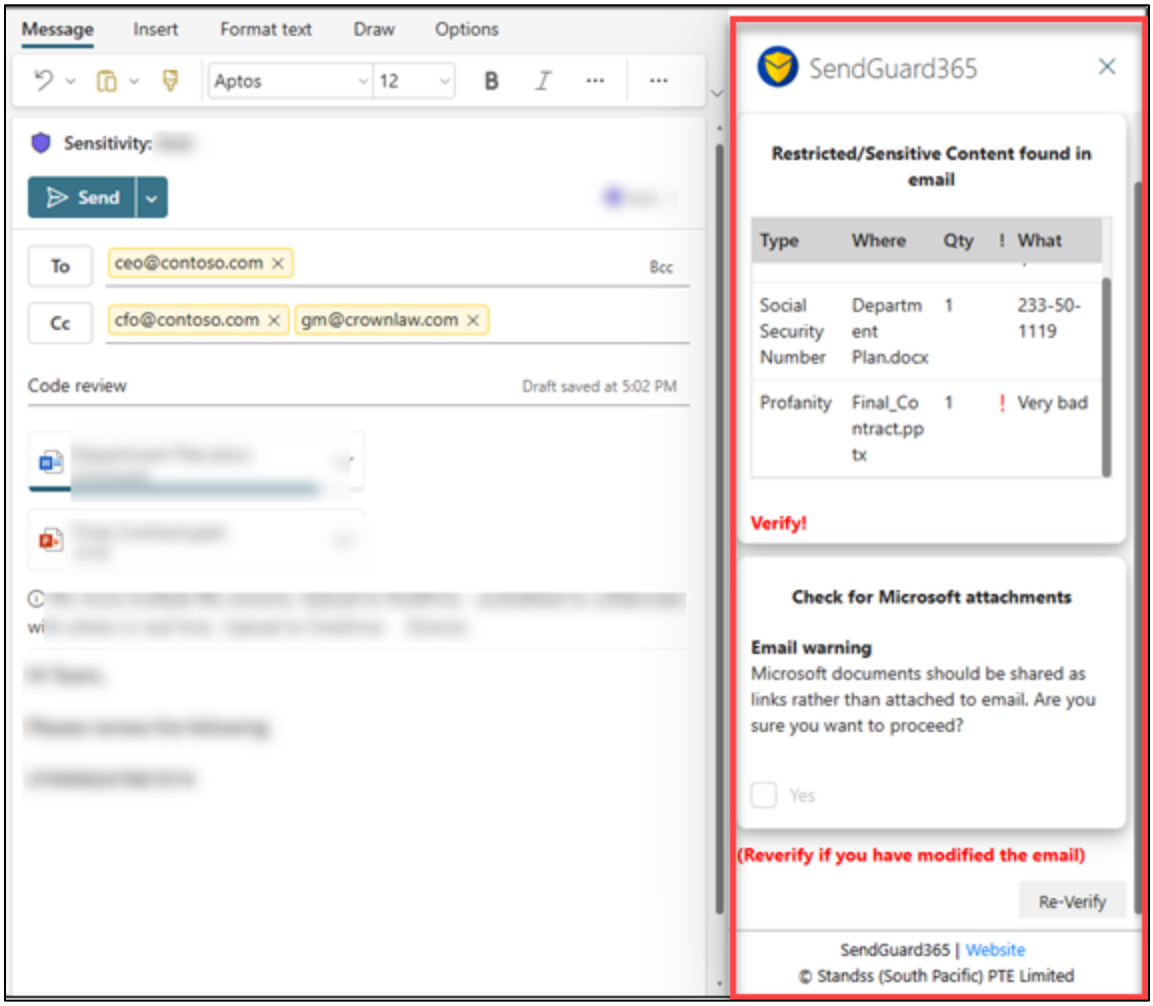
Ensure a standard of communication by preventing users from sending out emails with swear words etc.

Solution:

The **DLP component of SendGuard** was used to solve this problem. This component lets you define rules to perform your own checks on outgoing emails, and the resulting actions.

A list of PROFANITY WORDS was defined.

A rule was created to **scan outgoing emails** and **prompt users and block emails** when emails were found to contain any words in the Profanity Words List.



SendGuard is able to scan inside emails, meeting requests as well as common file types (Microsoft Office documents, PDF files etc.) sent as attachments.

The prompt also tells users what and where the detected words are so that they can make corrections before resending.

4. Warn users if email contains potentially sensitive or confidential information

Goal:

Notify (and get confirmation) from users before sending out emails with sensitive information such as credit card numbers etc.

Solution:

The **DLP component of SendGuard** was used to solve this problem. SendRules can be used to **scan emails for words or phrases using regular expressions**.

Regular expressions were used in this case to scan the email for credit card numbers so that the **user would be prompted for confirmation** before any emails with credit card numbers were sent out.

5. Delay (External) Emails to allow Unsend

Goal:

Give users the ability to change their mind and Unsend emails even after they have clicked Send.

Solution:

The **DelayGuard component of SendGuard** was configured to **delay emails for one minute in the Outbox** before the emails were actually sent out. This gave users the opportunity to go to the Outbox and cancel or change the email if they changed their mind.

DelayGuard can be setup to delay all emails, or only emails to specific email addresses (e.g. external emails).

The SendConfirm prompt (shown in Use Case 1 in this document) can also display a checkbox that can be used to bypass the delay and send urgent emails immediately.

6. Prevent emails from being sent to conflicting recipients

Goal:

Ensure that an email is not sent out to restricted combinations of recipients.

Background: Our customer was working with various sets of companies who were in competition with each other. They needed to ensure that the same email was never accidentally sent to a client and their competitor.

Solution:

The **SendRules component of SendGuard** was used to solve this problem. This component lets you define rules to perform your own checks on outgoing emails, and the resulting actions.

SendRules has a built-in rule condition to trigger if it detects a specified combination of recipients.

A list was created to identify the domains/recipients that should not be contacted in the same emails.

A rule was created to **prompt users and block emails** addressed to conflicting domains.

7. Include Attachments with Replies

Goal:

Improve productivity by automatically including attachments with replies.

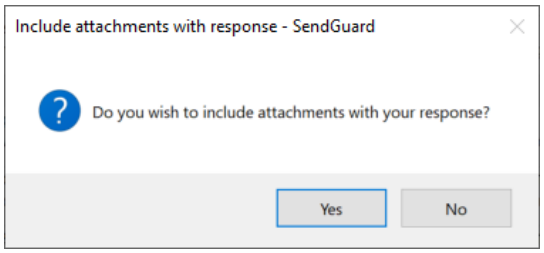
Background: A large law firm found that lawyers had to manually reattach files when responding to emails with attachments. The files needed to be reattached to the response because the responses were referring to information from the original attachment.

Solution:

The **ReplyGuard component of Send** was used to solve this problem.

ReplyGuard has an option to display the following prompt when replying to an email with attachments.

Now a user simply has to click **Yes**.



8. Encrypt Outgoing emails using Existing Server Software

Goal:

Give users an easier way to tell the server that this email needs to be encrypted.

Background: Our customer wanted to give users the option to encrypt emails directly from the SendConfirm prompt (shown in Use Case 1 of this document). They preferred this to displaying a separate prompt or using the checkbox on the Ribbon that users often forgot to use.

Solution:

The **SendConfirm prompt,** which is displayed to users before emails are sent out, was enhanced to include an Encryption checkbox. If the user ticks the checkbox, then the email is modified so that the server carries out the encryption before the email is sent out.

SendGuard is compatible with most server-based encryption software. If your organization does not use encryption software, then the checkbox can be hidden from the user.

9. Build Chinese Walls – Prevent groups of users from emailing each other

Goal:

Prevent the exchange of information between two departments because the exchange of information could potentially be considered insider trading (etc).

Solution:

The **SendRules component of SendGuard** was used to solve this problem. This component lets you define rules to perform your own checks on outgoing emails, and the resulting actions.

Users in each department were set up in separate distribution lists in Microsoft Exchange.

A rule was then created to **prompt users and block emails** whenever a sender in Distribution List (Department) A tried to send an email to any recipient in Distribution List (Department) B.

10. Use the correct Outlook (sender) account to send emails

Goal:

Ensure that emails are sent using the correct email account

Background: The customer was representing two major clients and doing most of the sales and support work on their behalf i.e. they were sending out sales and support emails on behalf of their clients. Each user had 2 Outlook email accounts (one for each of the clients). They had to ensure that the correct email account was used to send out the emails (depending on which client they were representing).

Solution:

The **SendRules and SendAccount components of SendGuard** was used to solve this problem. This component lets you define rules to perform your own checks on outgoing emails, and the resulting actions.

Rules were created to define which sending account should be used with which recipients.

If a user tried to **contact a customer or client using the wrong (sender) email account,** then they would be **prompted, and the email blocked**.

[Bonus Feature] Mass Marketing Risk Compliance

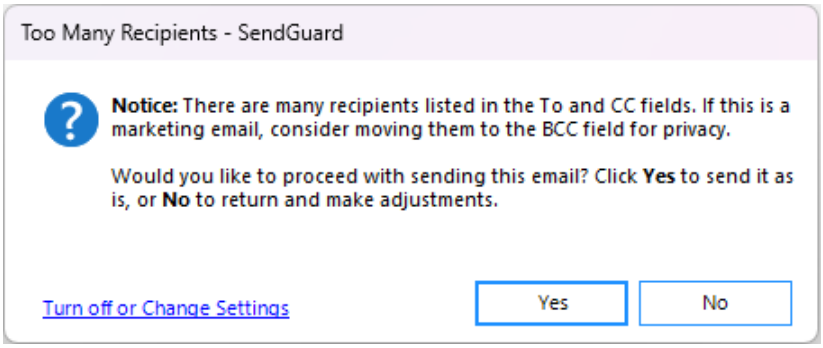
Goal:

Avoid accidental exposure of email addresses when emailing a large number of recipients.

Background: A Communications Manager was sending out a mass customer email with all the recipients populated in the "To" field. The Communications Manager had forgotten to put the email addresses in the "Bcc" field, thus exposing the email addresses of the recipients.

Solution:

SendGuard can warn and recommend BCC if email has too many recipients in the “To/Cc” field to mitigate unintentional unauthorised email address exposure. Ensure that emails with large recipient lists are sent securely preventing unintended visibility of email addresses.



Closing

The above use cases show how SendGuard’s various components can be configured and customized to provide organizations the email security and data leakage protection they need.

If you have specific requirements, please let us know (sales@standss.com).

Our team will help you with any customizations you need to achieve your organisation’s security requirements.

About SendGuard and Standss

Standss (South Pacific) Limited is a Microsoft Partner specialising in helping organizations with Microsoft Outlook.

Our clients include some of the world’s largest law and financial firms.

We have helped thousands of users in more than 50 countries over the last 15 years.

Please contact us at sales@standss.com for more information, an online demo or an onsite trial.