5 ways to reduce the risk of misdirected emails



When it comes to data breach prevention, the stakes are high. While phishing and ransomware attacks make headlines, misdirected email (emails sent to the wrong person or to the right person, with the wrong attachment) represents a much bigger threat.

58%

of people have sent an email to the wrong person while at work.

88%

of data breaches are caused by human error.

Misdirected emails are the most common error to cause a breach



To minimize risk, consider a specialized Governance, Risk & Compliance Solution for Outbound Emails and implement these best practices:



1 Confirm Recipients and Attachments

Autocomplete makes it too easy for Rachel Smith to get Rachael Jones' email.

Prompt users to review and confirm recipients and attachments before emails are sent and help prevent disclosure of confidential information!

2 Recall Emails

Ever wish you could unsend that email? Use **SendGuard** to configure a one to three minutes delay before your emails are sent. Allow your users to "recall" or "unsend" any emails even **after** they clicked "send" in case they find a mistake or change their mind.



3 Implement "Send Rules" to detect and act on sensitive content (DLP)

How can you ensure that your users are not accidentally (or intentionally) sending out sensitive or restricted information? You need to check!

Seek a solution with Data Loss Prevention (DLP) Content Scanning that can look inside emails, meeting requests and attachments like PDF and Microsoft Office documents to detect, warn and/or block.



Use a solution that supports custom rules to perform checks on outgoing emails and consider three important configuration scenarios:

Block Inappropriate Content

Ensure a standard of communication by preventing users from sending out emails with profanities, or inappropriate content.

Flag Confidential or Sensitive Information

Configure your solution to look for specific words or data patterns and warn/block users if it finds any potentially sensitive or restricted content (like credit card numbers).

Prevent Conflicts

Implement a virtual barrier to block the exchange of information between internal departments to create ethical boundaries, maintain confidentiality and prevent conflicts of interest.



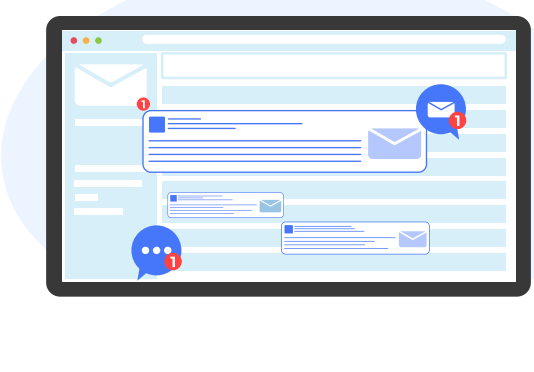
4 Include Attachments with Replies

Humans make mistakes. Manually reattaching documents increases risk and wastes time. Use a solution that prompts users to include original attachments in Replies.

5 Reduce "Reply-All"

Say no to the replyallpocalypses via indiscriminate use of "Reply All". Prompt users to review and confirm recipients when Reply All is clicked.

Ensure users are aware of exactly who they are sending emails to with tools like the **ReplyGuard** component of **SendGuard**.



Email mistakes don't have to become security incidents. Help protect your company from the risk of confidential information being emailed to the wrong people with Standss Governance, Risk & Compliance Solutions for Outbound Emails.

Trust SendGuard to detect and warn users about potential risks before emails are sent.

Talk to an expert!

Email: sales@standss.com | www.standss.com