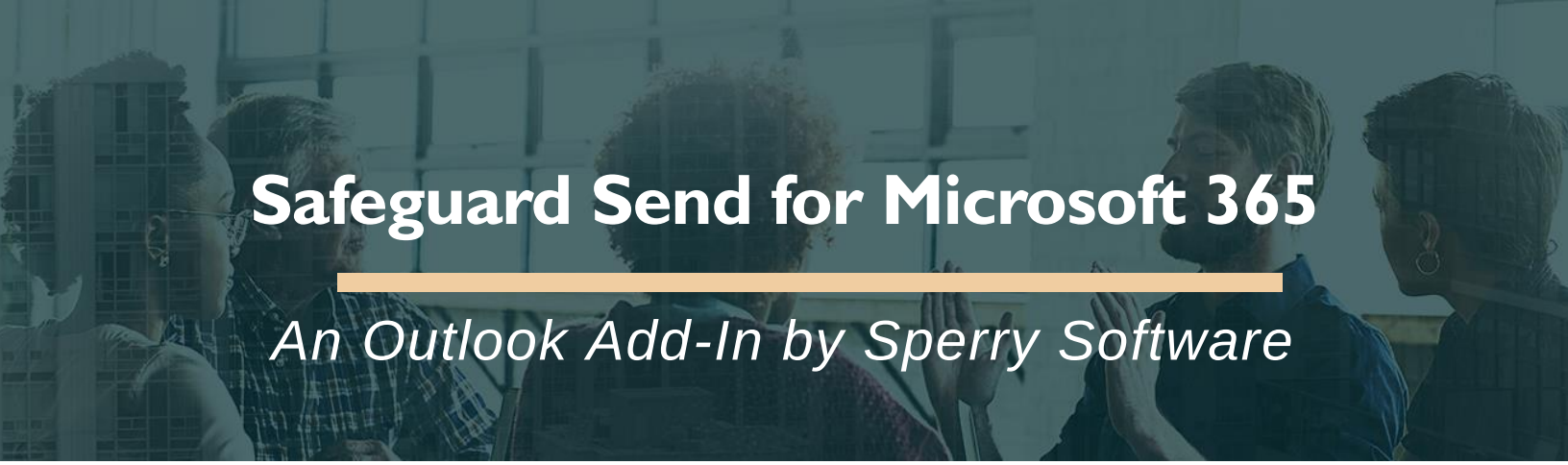

Safeguard Send for Microsoft 365

An Outlook Add-In by Sperry Software

Enhancing Email Security with Safeguard Send for Microsoft 365

This whitepaper explores the critical role of email security in modern enterprises and how Safeguard Send for Microsoft 365 can prevent costly email mistakes. It provides insights into the features, benefits, and implementation strategies for maximizing email security.

Contents

Introduction

For over 40 years, email remains a primary communication tool for businesses. In fact, it is a "matter of record", meaning that it serves as a formally and legally recognized account of events or facts. However, the risk of sending sensitive information to the wrong recipients poses significant security threats.

Figure 1 - Image of the Safeguard Send logo

This whitepaper examines these challenges and introduces Safeguard Send for Microsoft 365 as a robust solution.

Problem Statement

In today's fast-paced business environment, email remains a primary mode of communication. However, the sheer volume of emails sent daily increases the likelihood of human error. Users, being human, inevitably make mistakes, often due to being in a hurry or multitasking.

Here are some common scenarios leading to email mistakes:

1. Rushing to Complete Tasks:

Scenario: It's Friday afternoon, and an employee is eager to start their weekend. In their haste to send one last email, they might quickly fill out the recipients, attach a file, compose the body, and hit Send.

Consequence: They may accidentally attach the wrong file, potentially containing sensitive information that shouldn't be sent outside the company. This is especially problematic when replying to an email with external recipients.

2. Auto-Complete Errors:

Scenario: Outlook's Auto Complete feature saves the names and email addresses of recipients for quick reference. While this is a time-saver, it can lead to errors.

Consequence: A user might select the wrong name from the auto-complete dropdown list, especially if there are multiple addresses for the same name. This can result in sending emails to unintended recipients, leading to data breaches and confidentiality issues.

3. Misdirected Emails:

Scenario: The concept of sending an email to the wrong recipients is known as a misdirected email.

Consequence: According to Tessian, misdirected emails are a more significant problem than phishing, ransomware, and brute force attacks. In organizations with 1,000 employees, at least 800 emails are sent to the wrong person every year—equivalent to two a day. This can lead to data breaches, legal liabilities, and reputational damage.

4. Replying to BCC Emails:

Scenario: When a user replies to an email where they were included as a BCC recipient, their response can inadvertently reveal their inclusion in the conversation to all other recipients.

Consequence: This can compromise confidentiality, breach privacy agreements, and lead to awkward or damaging situations, especially in sensitive or competitive environments.

These scenarios and statistics underscore the critical need for robust email security measures. Safeguard Send for Microsoft 365 addresses these challenges by providing advanced features that help prevent common email mistakes, ensuring that sensitive information remains protected and compliance requirements are met.

Figure 2 - Sending emails is one of the easiest ways to violate corporate security

In our own statistics, we measure the number of times users go back and revise something – something that would have been sent out had they not been using the add-in – and users are revising emails 6.8% of the time. In a typical organization with 50 employees, each sending 10 emails a day (which may be too low a number), that's 34 emails getting revised *per day*.

Overall there are seven ways users can make mistakes when going to send emails:

Misdirected Emails

- Definition: Emails sent to the wrong recipients, often due to autocomplete errors or selecting the wrong contact.
- Impact: Can lead to data breaches, exposure of sensitive information, and compliance violations.

Wrong Attachments

- Definition: Sending incorrect or unintended attachments.
- Impact: Exposure of confidential or sensitive data, potential legal issues.

Using To/CC Instead of Bcc

- Definition: Exposing email addresses by using To or Cc fields instead of Bcc.
- Impact: Breaches of privacy, potential legal issues, and exposure of confidential information.

Non-Compliant Emails

- Definition: Sending emails that do not comply with legal or regulatory requirements.
- Impact: Legal penalties, financial losses, and reputational damage.

Sending Emails with PII

- Definition: Sending emails with Personally Identifiable Information such as SSNs, credit card numbers and other account numbers.
- Impact: Violations (especially GDPR) can lead to large legal penalties, financial losses, and reputational damage.

Replying To All

- Definition: Replying to emails with the Reply To All button includes everyone in the reply, even if the email is sent to the entire company.
- Impact: Slowdown in productivity as each employee reads the response. In some cases, repeated use of the reply all chain can also bring a server to a crawl.

Replying When BCC'ed

- Definition: When a user replies to an email where they were included as a BCC (Blind Carbon Copy) recipient.
- Impact: Compromised confidentiality, breach of privacy agreements, and can lead to litigation, especially in sensitive or competitive environments.

Solution Overview

Safeguard Send for Microsoft 365[1] offers advanced features such as external domain warnings, restricted email/domain warnings, and sensitive content detection. These features help prevent misdirected emails and enhance overall email security by getting users to *think* before they make a mistake when sending emails. It can be thought of as an additional layer in your email security posture, giving users a second chance to correct any issues before the email goes out. Key features of the add-in include:

1. **External Domain Warnings**: The add-in prompts users when they are about to send an email outside the company, helping prevent accidental disclosure of sensitive information to external parties. This reduces the risk of accidental data leaks and ensures sensitive information remains within the organization, thereby enhancing data security and compliance with privacy regulations.

2. **Restricted Email/Domain Warnings**: Users receive warnings when attempting to send emails to specific restricted email addresses or domains, reducing the risk of unauthorized communication. This helps prevent unauthorized communication and potential data breaches, ensuring that sensitive information is only shared with approved recipients, thus maintaining the integrity and confidentiality of corporate communications.

3. **Sensitive Content Detection**: The solution can identify and flag emails containing sensitive information such as social security numbers, credit card details, or custom-defined keywords in the subject, body, or attachments. This protects against inadvertent sharing of confidential

[1] Sperry Software – Safeguard Send for Microsoft 365

information, reducing the risk of data breaches and compliance violations, and safeguarding the organization's reputation and legal standing.

4. **Multi-Domain Recipient Check**: Alerts users when they are sending to recipients from multiple external domains, preventing potential data breaches. This minimizes the risk of cross-domain data leaks, ensuring that sensitive information is not inadvertently shared with unauthorized parties, thereby enhancing overall email security.

5. **Attachment Controls**: Warns users if the number of attachments exceeds a defined maximum or if attachment names or content are questionable. This helps prevent the accidental sharing of inappropriate or excessive information, ensuring that only necessary and relevant attachments are sent, which reduces the risk of data breaches and maintains professional communication standards.

6. **Customizable Rules and Actions**: Administrators can set up various conditions and actions, such as adding a BCC or modifying the email subject or body, based on specific triggers. This allows for tailored email security policies that meet the specific needs of the organization, enhancing flexibility and control over email communications, and ensuring that security measures are aligned with corporate policies.

7. **White Labeling Options**: Allows for complete customization of the warning prompts with corporate logos, fonts, and colors, ensuring a consistent brand experience. This ensures a consistent brand experience for users, reinforcing corporate identity and professionalism in all email communications, and enhancing user trust and engagement with the security measures.

8. **Centralized Dashboard**: Offers a centralized management interface for setting up and monitoring rules across all users, simplifying administration for IT teams. This simplifies the administration and enforcement of email security policies, providing IT teams with a streamlined and efficient way to manage and monitor email security, which enhances operational efficiency and reduces administrative overhead.

9. **Reporting Features**: Captures data on email activity, including email sends and revisions, and provides detailed reports. This allows managers to gain valuable insights into email usage patterns, identify potential training needs, and measure the effectiveness of email security policies. By understanding how often users revise their emails after being prompted,

organizations can demonstrate the value of the add-in, justify its expense, and continuously improve email security practices.

10. **Easy Deployment**: As a modern Outlook add-in, it can be quickly deployed across an organization without the need for individual desktop installations. This reduces the time and resources required for deployment, ensuring a swift and seamless implementation of the email security solution, which minimizes disruption to business operations and accelerates the realization of security benefits.

These features work together to create a robust email security solution that helps organizations prevent common email mistakes, comply with data protection regulations, and maintain professional communication standards. By prompting users to review their emails before sending, Safeguard Send for Microsoft 365 adds a crucial layer of security and mindfulness to the email communication process.

Implementation Strategy

Implementing Safeguard Send for Microsoft 365 involves a straightforward setup process, and basically consists of three steps (sign-up, deploy, create/edit your rules). This section outlines the steps for installation, configuration, and user training to ensure a smooth deployment. That said, there are several points to consider when implementing a change to the normal email flow for users.

Plan Your Rules

Plan ahead - before implementing Safeguard Send for Microsoft 365, it's important to plan ahead. You should begin by deciding which rules you are going to implement along with the actions. Safeguard Send for Microsoft 365 comes with a dashboard that allows you centralized control over the add-in for yourself or your entire company. You can also customize the text of the warning prompt, add a BCC recipient, or prevent the email from being sent until the user corrects the mistake. A vision for what you want to accomplish with the add-in is important in this step.

Plan Your Deployment

You will also want to consider when to uninstall the original desktop version, keeping in mind that if both the desktop version and the new Microsoft 365 version are installed, then the users will see two warning prompts. At the same time, be aware that deployment from the Microsoft Admin Center can take anywhere from 24-48 hours before users begin seeing the warning prompt according to this article from Microsoft.

Plan Your Communications To Users

Next you will want to identify the users who will be affected by the migration and begin to communicate with them about the changes. What are you going to tell your users?

In general, like all good communication, you will want to let them know about changes that are coming (and when) and what to expect (like side by side screenshots of the original Safeguard Send prompt and a sample of the new Safeguard Send for Microsoft 365 prompt), then let them know about what's currently happening (as it is deployed), and a final communication after deployment to let them know that it is now deployed, what to expect when they send an email and how to handle any issues going forward.

These three communications (before, during and after deployment) serve as important training for your users on how to use the add-in. It can be useful to provide users with a link to a corporate page that has helpful information like what to do if you can't send an email, what to do if you were (or were not) prompted when you supposed to be (or not), and how to get in touch with IT regarding issues with the add-in.

Test, Test, Deploy

Before deploying the new version of Safeguard Send for Microsoft 365, it's important to test it in a non-production environment. This will help you identify any issues or conflicts that may arise during deployment. In fact, in general it's best to implement a three phase deployment.

1) In the first phase, start with a small team of users who are well versed in what to expect when using the new version of the add-in so that if anything unexpected occurs, they will be able to notice and have the ability to take action. If you are planning on using the reporting feature, it is during this phase that you would want to check the reports being generated in the dashboard to make sure that you are getting good actionable results.
2) After a time, the testing team can be expanded to include even more users or even a single department or branch in a second phase. It is during this second phase that you will want to identify any potential areas of concern for example, departments using a different domain or anyone using any in-house macros or other vendor add-ins (especially when sending emails).
3) Finally in the third phase, the deployment to all users can occur (keeping in mind the communications to all users in the Plan Your Communications step above).

Data and Research

These statistics highlight the prevalence of email-related security issues and the importance of implementing robust email security measures. They demonstrate the significant impact of misdirected emails, phishing attacks, and other email-related security incidents on organizations.

1. In organizations with 1,000 employees, at least 800 emails are sent to the wrong person every year. That's approximately two misdirected emails per day.
2. In 74% of breaches, human factors played a role, encompassing social engineering tactics, mistakes, or misuse.
3. 95% of Cybersecurity leaders admit to feeling 'stressed' about email security.
4. 91% of organizations experience outbound email security incidents caused by data loss and exfiltration, and 94% were adversely affected by them.
5. 58% of organizations had to cease operations following breaches of internal information barriers by email.
6. Remarkably, 6.8% of users who are prompted by Safeguard Send for Microsoft 365 when they send an email go back and revise something in their email (recipients, attachments, subject or body text). This data, aggregated across all users of the add-in, demonstrates significant engagement with the add-in's prompts. It highlights the effectiveness of the solution in encouraging users to double-check their emails, thereby preventing potential mistakes and enhancing overall email security.

Conclusion

Safeguard Send for Microsoft 365 is a powerful tool for enhancing email security. By implementing this solution, organizations can significantly reduce the risk of misdirected emails and protect sensitive information. To learn more about Safeguard Send for Microsoft 365 and how it can benefit your organization, visit our website or contact our sales team at sales@sperrysoftware.com.