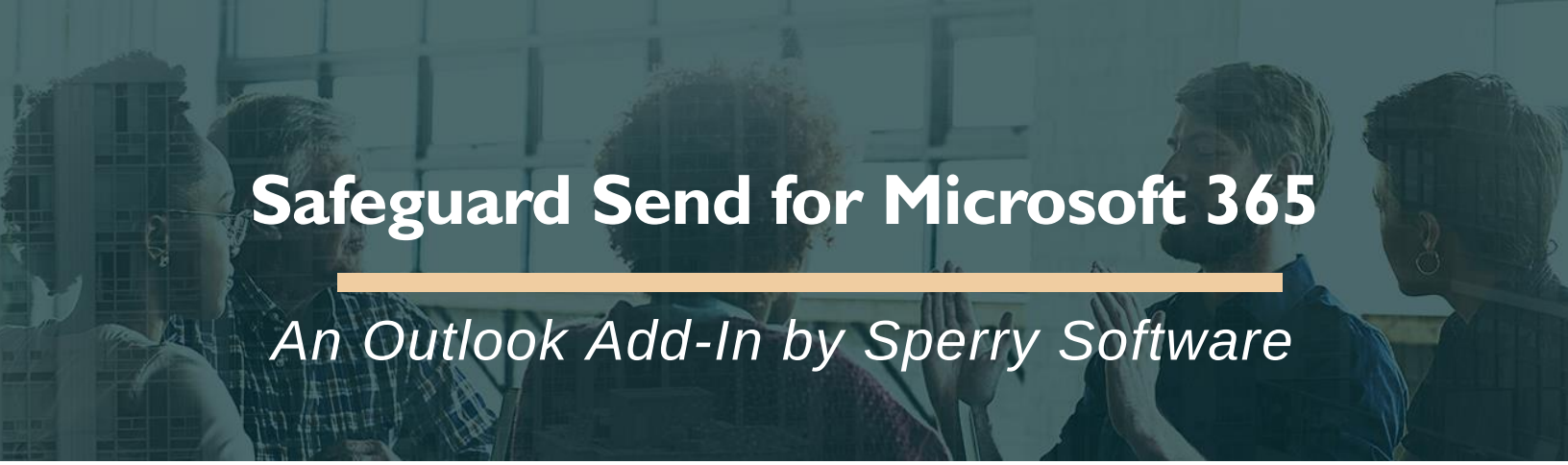

Safeguard Send for Microsoft 365

An Outlook Add-In by Sperry Software

Enhancing Email Security with Safeguard Send for Microsoft 365

Summary: 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 significantly increases the likelihood of human error. As users navigate their busy schedules, they sometimes rush through tasks or multitask, inadvertently making mistakes that can have serious consequences.

For instance, on a Friday afternoon, an employee excited to start their weekend might hastily send out an email without taking the time to verify the recipients or attachments. This haste can lead to accidentally including the wrong file—potentially containing sensitive information that should not leave the company—especially when replying to threads that include external contacts.

Auto-complete features in Outlook, while convenient, can exacerbate this issue. Users may mistakenly select the wrong contact from a dropdown list, resulting in emails being sent to unintended recipients and compromising confidentiality. Furthermore, misdirected emails are alarmingly common. Research by Tessian indicates that in organizations with 1,000 employees, at least 800 emails are incorrectly sent each year—translating to roughly two per day. This not only risks data breaches but can also expose organizations to legal liabilities.

Particularly concerning is the act of replying to BCC recipients. A user who replies can inadvertently disclose their inclusion to other recipients, which jeopardizes privacy and confidentiality in sensitive situations. Such scenarios illustrate the critical need for robust email security measures.

Safeguard Send for Microsoft 365 directly addresses these challenges with its suite of advanced features designed to prevent common email mistakes, ensuring sensitive information is protected and compliance requirements are adhered to. According to our findings, users are revising their emails 6.8% of the time after receiving prompts from the add-in—a significant behavior change that demonstrates engagement with security measures. In a typical organization with 50 employees sending 10 emails each day, this equates to an impressive 34 revised emails daily, reinforcing the value of implementing effective email safeguards.

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

These examples highlight the importance of implementing comprehensive email security solutions to mitigate the risks associated with human error. By addressing these common pitfalls, organizations can protect their sensitive information, maintain compliance, and safeguard their reputation.

Failing to double-check emails before sending them can lead to significant risks and consequences for any organization. A single misdirected email can result in a data breach, exposing sensitive information to unauthorized recipients and potentially violating privacy regulations. This, in turn, can lead to severe legal liabilities, including fines and penalties, as well as costly litigation. Beyond the immediate financial impact, such incidents can cause long-term reputational damage, eroding trust with clients, partners, and stakeholders. The fallout from these mistakes can disrupt business operations, divert resources to damage control, and ultimately harm the organization's bottom line. Therefore, implementing robust email security measures and encouraging users to double-check their emails are crucial steps in mitigating these risks and protecting the organization's integrity.

Here are some common scenarios users encounter leading to email mistakes:

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

Figure 3 - Getting users to think before they hit send is the goal

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

Figure 4 - Ensuring compliance: Safeguard your communications with robust email security measures

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

Planning ahead is crucial before implementing Safeguard Send for Microsoft 365. Begin by deciding which rules to implement and the corresponding actions. Safeguard Send for Microsoft 365 includes a dashboard that provides centralized control over the add-in for an individual or the entire company. The text of the warning prompt can be customized, a BCC recipient can be added, or the email can be prevented from being sent until the mistake is corrected. Having a clear vision for what needs to be accomplished with the add-in is important at this stage.

Plan Your Deployment

Consideration must also be given to when the original desktop version should be uninstalled. If both the desktop version and the new Microsoft 365 version are installed simultaneously, users will encounter two warning prompts. Additionally, it is important to be aware that deployment from the Microsoft Admin Center can take anywhere from 24 to 48 hours before users begin seeing the warning prompt, as noted in an article from Microsoft.

Plan Your Communications To Users

Next, identify the users who will be affected by the migration and begin communicating with them about the changes. What information will be conveyed to the users? In general, effective communication involves informing them about the upcoming changes (and when they will occur) and what to expect (such as side-by-side screenshots of the original Safeguard Send prompt and a sample of the new Safeguard Send for Microsoft 365 prompt). Additionally, provide updates during the deployment process and a final communication after deployment to inform them that it is now complete, what to expect when sending an email, and how to handle any issues going forward.

These three communications (before, during, and after deployment) serve as important training for users on how to use the add-in. It can be useful to provide users with a link to a corporate page that includes helpful information such as what to do if an email cannot be sent, what to do if a prompt was (or was not) received as expected, and how to contact IT regarding issues with the add-in. This approach ensures that users are well-informed and comfortable with both the old and new systems, facilitating a smooth transition.

Test, Test, Deploy

Before deploying the new version of Safeguard Send for Microsoft 365, testing in a non-production environment is crucial. This process helps identify potential issues or conflicts that may arise during deployment. A three-phase deployment strategy is generally recommended:

1) The initial phase involves a small team of users well-versed in the new version's functionality. Their expertise allows for quick identification and action on any unexpected occurrences. If the reporting feature is to be utilized, this phase is ideal for verifying the dashboard reports to ensure actionable results are being generated.

2) The second phase expands the testing team to include more users or a specific department or branch. This stage is critical for identifying potential areas of concern, such as departments using different domains or the use of in-house macros or other vendor add-ins, particularly when sending emails.

3) The final phase involves deployment to all users, keeping in mind the importance of communication as outlined in the Plan Your Communications step. This ensures a smooth transition for the entire organization.

This phased approach minimizes risks and ensures a well-prepared user base for the transition to the new system.

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. Safeguard Send for Microsoft 365 has a reporting feature that allows for management to easily identify users who most frequently go back and revise something and why.

Measuring Value

Safeguard Send for Microsoft 365 is a powerful tool for enhancing email security. But executives and managers need to know that the product is delivering the value they need. Safeguard Send for Microsoft 365 provides valuable insights to help understand and improve your organization's email practices. Here’s how IT Admins and managers can make the most of this data:

Key Metrics

• Email Revision Rate: Track how often users revise emails after being prompted. High rates indicate vigilance, while low rates may suggest careful initial composition or disregard for prompts.

• Email Send Rate: Understand your team's email volume and identify key communicators.

• Revision Percentage: See the proportion of emails that are revised, helping to identify potential training needs.

• Common Revisions: Discover which elements (recipients, attachments, subject, body) are most frequently revised.

Additional Insights

• Time to First Revision: Measure how quickly users respond to prompts.

• Revision Impact: Categorize revisions by their impact to highlight the add-in's effectiveness.

• User Engagement with Prompts: Identify users who may need additional attention based on their interaction with prompts.

• Industry Benchmarks: Compare metrics with industry averages and overall averages (that is, across all users of the add-in) to gauge performance.

By leveraging these insights, managers and executives can better understand their team's email practices, identify areas for improvement, and demonstrate the value of Safeguard Send for Microsoft 365 in enhancing email security and efficiency. These enhancements will help managers see the value of the add-in more clearly and provide actionable insights to improve email practices within their organization.

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.