Reduce accidental data leakage

Solve the problem of misaddressed emails with VIPRE SafeSend

Have you ever mistakenly sent an email to the wrong person? A misaddressed email can be embarrassing, but misaddressed emails containing sensitive information can be even worse. Data breaches caused by misaddressed emails can result in regulatory non-compliance, costly fines, and may even require litigation.

Use VIPRE SafeSend to confirm external recipients and attachments in Microsoft Outlook when sending emails
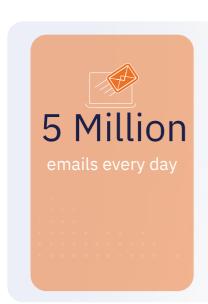
VIPRE SafeSend is an Outlook and OWA add-in that prevents misaddressed emails or inadvertent auto complete email
mistakes. VIPRE SafeSend requires the user to confirm external recipients and file attachments before an email can be sent.

VIPRE SafeSend also scans outgoing emails and attachments to make sure sensitive data does not leave your network. Build your own DLP rules to detect sensitive keywords or data patterns. With regular expressions, detect Personally Identifiable Informatio (PII) or any kind of structured data.

With VIPRE SafeSend you can:

- Confirm external recipients in emails, meeting invitations and task requests
- Proactively help users prevent accidental data leakage due to autocomplete and reply-all errors
- Create a white-label version with your corporate logo and style for seamless integration
- Keep your data in-network. VIPRE SafeSend is a security- first solution which does not require any data to leave your organization. All data remains on your network. Specify per-user or per-group settings
- Deploy to tens of thousands of users using Group Policy, SCCM, or any other deployment tool. No limitation in terms of user count.
- Log all events with a full audit trail stored locally or centrally
- Support Outlook local languages
- Add DLP functionality to automatically scan outgoing emails and encrypted attachments simultaneously to reduce the risk of a sensitive data leak

5 Million
emails every day

300+
enterprises

425,000+
active users

Book your demo today

Key Benefits

Market leading technology	More than 425,000 active users across more than 300 enterprises.
Prevents spear phishing	Spoofed email addresses are caught before replies can be sent. Replying to a spear phishing email displays the VIPRE SafeSend confirmation window highlighting the external email address.
Improves awareness	VIPRE SafeSend keeps security front-of-mind at all times. It can be customized to include your corporate branding and custom text with links to your security policies. Require users to open attachments before being able to send them.
VIPRE Email Security Encryption Integration	VIPRE SafeSend is designed to work with VIPRE Email Security Encryption as well as many other third party encryption services. The tool can prompt users to encrypt emails which contain particularly sensitive data by asking them if they would like to encrypt the email.
GDPR compliant	The preventative function of VIPRE SafeSend aligns with GDPR Article 32 "to implement appropriate technical and organizational measures together with a process for regularly testing, assessing and evaluating the effectiveness of those measures to ensure the security of processing."
PC and Web Add-Ins	VIPRE SafeSend is available for PCs and Macs. The PC add-in operates on Windows devices, whereas the web add-in extends coverage to Outlook for Mac and Outlook Web Access.

Action options

VIPRE SafeSend actions can be triggered under different conditions. The most common option is to display VIPRE SafeSend for all external emails being sent outside the company. The second most common option is to display it only when files are sent externally.

VIPRE SafeSend can also be configured to trigger only when there is a DLP match in an external email. This is useful if you have defined specific DLP rules and only want to inform the user of matches for any of those rules.

System requirements

System Component SafeSend PC Add-in	System Component SafeSend Web Add-in
Minimum Requirement **Operating Systems** Windows 10, 8.1, 8, 7 Windows Server 2016, 2012, 2008 R2 **Email Clients** Outlook 2019, 2016, 2013, 2010 Both 32-bit and 64-bit versions .NET Framework 4.7, 4.6, 4.5, 4.0 Microsoft .NET 4.7.2 or later is required to be installed but all newer versions of Windows already have this included Please note that .NET 4.7.2 Client Profile is not sufficient to install SafeSend and that the full version of .NET 4.7.2 or later is required	**Minimum Requirement** .NET Core 6.0 capable web server Hosting Bundle is required when using IIS Server (Recommended) **Microsoft 365** - Email Clients: Outlook for Mac v16.30+, Outlook for Windows 2019, 2016, Both 32-bit and 64-bit versions **Browsers for OWA** - Mozilla Firefox, Google Chrome, Microsoft Edge, Microsoft Edge Chromium, Internet Explorer 11, Safari **Exchange 2019** - Email Clients: Outlook for Windows 2019, 2016, Both 32-bit and 64-bit versions **Browsers for OWA** - Mozilla Firefox, Google Chrome,Microsoft Edge, Microsoft Edge Chromium, Internet Explorer 11

Optional DLP module

VIPRE SafeSend with DLP further scans attachments and email content for particularly sensitive data and allows companies to build additional custom DLP rules. Using regular expressions, you can detect sensitive keywords or data patterns inside the email body or attachments such as credit card numbers, bank account details, or social security numbers. The DLP add-on is available for both the PC and web add-ins.

- Define a list of client keywords and approved domains.
- Prevent client data being sent to the wrong client.
- Give users a warning when sending to a non-approved domain.
- Stop specific information from going to non-approved domains.
- Apply company DLP rules to password protected files before sending.
- Enforce company policies by ensuring users password protect files.
- Scan emails for Microsoft Information Protection labels and require additional verification.

ABS Technology