Essential How-To Guide

Prevent Accidental Emailing





TABLE OF CONTENTS

Top Email Security Threats	4
Causes of Accidental Emailing	6
Consequences of Data Breaches	.10
Preventing Email Data Loss	.12
VIPRE SafeSend: How Email DLP Works	.13
Choosing and Installing an Email DLP Solution	.16
Conclusion	.17



Did You Just Send an Email to the Wrong Person?

Let's face it, we've all done it. If you're lucky, you can correct that mistake with a follow-up note that apologizes and asks the unintended recipient to delete the erroneous message (along with any attached files) ASAP.

But often it's too late for that, and the consequences can be disastrous—from substantial fines to irreparable damage to your enterprise's reputation that can lead to canceled customer contracts and eventual layoffs. All of these fallouts can quickly spiral out of your control, simply because you or someone in your organization forgot to double-check each recipient's email address before clicking "Send."

NO ORGANIZATION IS IMMUNE TO HUMAN ERROR

It's not just your imagination, there appears to be a steady stream of security breaches in the news. One report explains how the personal identifiers of global political leaders have been accidentally disclosed, another story details a hospital that has inadvertently revealed the personal details of hundreds of patients, and still another article chronicles how a city council shared confidential information about thousands of children and adoptive parents.

All of these examples have one thing in common: accidental emailing.

Think your enterprise is immune? Think again—one of your employees may actually have sent dozens of messages to the same wrong recipient without even knowing it. That's what happened with a confidential military agreement between two prominent countries, which went public when someone reported receiving "a lot of emails targeted to a different person with the same name."

The key takeaway? Your organization could reveal confidential information (contracts, ongoing negotiations, intellectual property, trade secrets, personally-identifiable information) in any of the 40 emails sent on average by each of your employees every day.

In this e-book you'll get a closer look at data breaches and misdeliveries via email, and learn how companies can implement security measures to prevent accidental emailing by using an email data loss prevention (DLP) solution.

TOP EMAIL SECURITY THREATS

Email is the backbone of modern corporate communications, and the most popular digital medium in the world. 3.7 billion users send 269 billion emails every day—representing three times the global daily messaging traffic of Facebook, WhatsApp, and SMS combined. Running an organization without email is unthinkable, especially as employees become more mobile and work remotely from home or at clients' sites, often in different time zones.

Fortunately, today's enterprises and their employees benefit from some level of security when using email. For example, authentication and encryption protocols are commonplace. In addition, communications can be centrally governed by corporate information security policies. Furthermore, IT administrators control the allocation of corporate email addresses, and thus can remotely wipe any device that is lost, stolen, or retained by an employee leaving the organization.

Regardless of these security capabilities, companies still remain vulnerable to a variety of cyber threats and data breaches that can plague email, including hacking, malware, phishing, spoofing, and misdeliveries.

NOTABLE STATISTICS ON EMAIL SECURITY THREATS

1 Email phishing is the #1 type of threat action in breaches

94% Detected malware was delivered via malicious email attachment

Social media attacks featured phishing emails

Misdeliveries represent approximately 60% of healthcare security errors

1 Source: Verizon's 2019 Data Breach Investigations Report; https://enterprise.verizon.com/en-gb/resources/reports/dbir/

TOP EMAIL SECURITY THREATS

HACKING

Email hacking consists of the unauthorized access and manipulation of a user's email account and messages, and is a common organizational threat according to the Verizon 2019 Data Breach Investigations Report. The report states that for the top hacking action vectors in breaches, 60% of the time the compromised web application vector was the front-end to cloud based email servers; such hacking is usually linked to stolen or weak passwords.

MAI WARF

Malware can be broken down into different categories, often infecting computers or networks via attachments in malicious emails. With ransomware hackers can lock their victim's computer, demanding money in exchange for a decryption key. But the damage malware can inflict goes far beyond ransoms. Spyware, for example, can collect key personal information—passwords, usernames, social security numbers—and reveal it to a variety of third parties (including your competitors) for months without you knowing you've been compromised.

PHISHING & SPOOFING

Hackers may also try to trick your employees by presenting themselves as someone trustworthy. Wouldn't they be tempted to execute a request coming from your CEO, asking for an urgent wire transfer to purchase business plane tickets or complete a time-critical project? Demands like that certainly appear legitimate and thus are often complied with, which is why business email compromise (BEC) scams continue to be popular with cybercriminals.

MISDELIVERIES

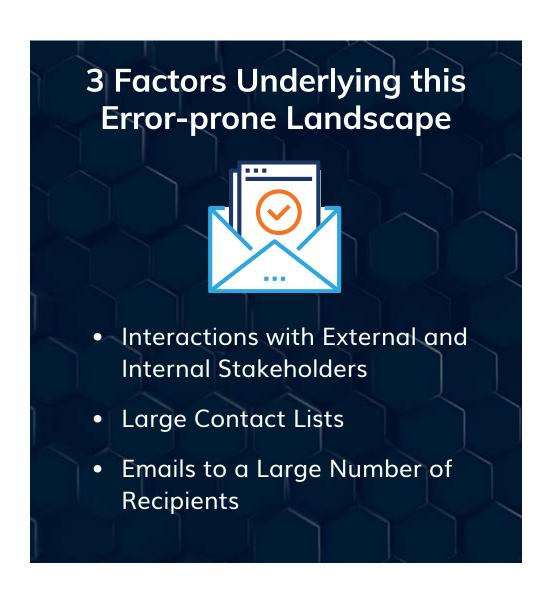
The threats discussed so far all have the intent to harm your enterprise deliberately—and they all originate externally. The media love to report these types of attacks, and organizations invest a sizeable portion of their enterprise IT security budget to fight them. By contrast, unintentional security incidents don't receive the same attention—but that doesn't make them any less dangerous. In fact, human errors (including misdeliveries via email) are almost twice as likely to result in a confirmed data disclosure.

In fact, human errors (including misdeliveries via email) are almost twice as likely to result in a confirmed data disclosure.

CAUSES OF ACCIDENTAL EMAILING

DID YOU KNOW THAT 52% OF ORGANIZATIONS CHARACTERIZE **INSIDER THREATS AS UNINTENTIONAL?**²

Such errors can be attributed to busy staff, constantly on the move or juggling deadlines and deliverables. Employees strive to work better and faster, but sometimes they don't spend enough time verifying whether each recipient's email address is correct. In their defense, today's employees function in a business landscape that fundamentally makes mistakes more likely.



2 Unintentional Insider Threats: A Foundational Study; CERT Insider Threat Team. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=58744

FACTOR #1: INTERACTIONS WITH EXTERNAL & INTERNAL STAKEHOLDERS

Do you outsource some of your organizational processes, whether to cut costs or to help you maintain focus on core business functions? Are you planning to scale operations domestically or abroad? Are you communicating with many potential candidates to hire the best talent? If so, your staff is likely sending a multitude of emails to external stakeholders—often with attachments that potentially contain personally-identifiable information and intellectual property.

While that is obviously alarming, sending sensitive data to the wrong recipient(s) within your enterprise can be equally harmful. Imagine how risky it would be if all your employees became aware of a confidential new product that your R&D team has been developing. What if a Human Resources officer inadvertently divulges detailed information on employee compensation plans?

Such risks span a wide variety of departmental functions within a typical organization, as detailed in the following table:

Activities Prone to Security Breaches via Accidental Emailing

Department	Functions
Purchasing	 Sourcing, purchasing and exchanging info with multiple suppliers Managing bidding processes with detailed instructions, multiple files Negotiating extensive sourcing contracts with different stakeholders
Sales	 Working with multiples files (e.g., sales collaterals, RFPs, pricing info) Negotiating extensive customer contracts with dozens of clients, requiring confirmation from multiple internal stakeholders
Customer Service	 Managing personal details of numerous customers every day Collecting, sending personally-identifiable information via forms Different agents serving same customer, sharing access to private files
Marketing	 Working with external agencies and media on marketing campaigns Organizing events and orchestrating logistics with various suppliers
R&D	 Sending blueprints and plans to legal department to obtain patent for breakthrough technology Exchanging confidential info with external partners to design, manufacture new products
Legal	 Managing thousands of documents containing trade secrets and commercial information Supporting entire departments on all legal queries, relevant documents

FACTOR #2: LARGE CONTACT LISTS

As a natural part of their job duties, your employees access and build large contact lists with hundreds or thousands of recipients. How likely is it that they will come across different people with the same or confusingly similar names? Consider what could happen when employees deal with only two variants—James Smith and Jane Schmidt—in these hypothetical scenarios.

Same Names in Different Companies

A sales manager working at Company A wants to add three salespeople to her team, and thus works with an HR officer named James Smith to discuss future job responsibilities, manage potential candidates and agree on salary packages. Coincidentally, there is another James Smith in the sales manager's contact list who works for another organization—Company B.

An error could easily happen in this situation. For example, the sales manager might put the wrong James in CC and email him a list of shortlisted candidates—which he can then use to fill vacancies for the same or similar roles at Company B! Or she might reveal valuable information about Company A's strategy and compensation policies. Beyond looking unprofessional, this error could pose a serious threat to Company A.

Same Names within the Same Company

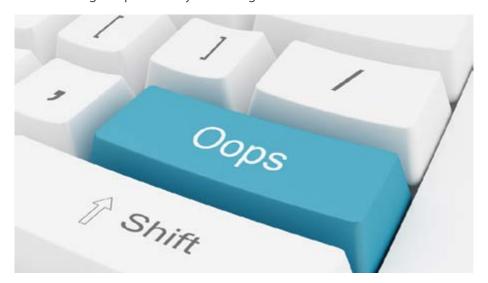
Building on the example above, imagine there is a sales associate at Company A who has been underperforming lately, and his name also happens to be James Smith. The sales manager is considering various ways to address this problem, including finding the ineffective sales

associate a new job in another department. She sends several emails to James Smith—Company A's HR officer—on that topic to discuss what to do.

That is obviously a very sensitive conversation, and the last thing the sales manager wants is to get the two recipients confused. If that happens she would inadvertently alert James—her direct report, who is not fully aware of his tenuous job status—about her concerns. Not only would this demoralize him, it could also potentially affect the performance of everyone else on the sales team.

Similar Names within the Same Company

Company A hires a new Chief Security Officer named Jane Schmidt; the sales manager has not yet met Jane personally, but would like to make a positive first impression on her when she has the chance. If the sales manager tries to send an email with personally-identifiable information to James Smith (the HR officer) but mistakenly sends it to Jane Schmidt instead, it's a safe bet Jane will never forget or trust the sales manager—potentially hindering her career advancement.



FACTOR #3: EMAILS TO LARGE NUMBER OF RECIPIENTS

Some departments in your company may need to send strategic communications via email to a large number of recipients. This might include informing entire divisions about changes in senior leadership teams, or giving some internal recognition to people who have contributed to signing a massive deal.

Large-scale updates like these are often achieved using bulk emails, with so many addresses in the TO, CC and BCC fields that human errors (e.g., adding unintended recipients or misspelling names) become virtually unnoticeable. The chances are that no one will carefully check to ensure every recipient's details are accurate on these huge lists—thus exposing your enterprise to risk.

Another danger is the misuse of CC and BCC. For example, you could disclose the contact details of your entire employee or client base if you use the wrong field, potentially giving your competitors a golden opportunity to lure your customers away and recruit your employees.



CONSEQUENCES OF DATA BREACHES

It is difficult to predict what the exact consequences of a given breach could be. Deloitte published a report³ that takes an in-depth look at the various business impacts that may occur when confidential records are lost or stolen. The study makes an important distinction between direct costs (which companies incur shortly after an incident) and hidden costs (which have long-lasting effects). The repercussions from these latter costs may account for 90% of the total business impact including financial, reputational, and intellectual property damages.

SHORT-TERM FINANCIAL COSTS

If your company is responsible for a breach, you'll need to allocate the resources and time needed to remediate the situation. This begins with a thorough technical investigation to find out what happened, identify security holes, and manage any external communications. You then must take immediate actions to notify and protect individuals at risk, as well as secure faulty systems and processes.

LONG-TERM FINANCIAL COSTS

The real financial costs only surface later on. For example, your enterprise will probably need to pay penalties, along with attorney and litigation expenses. Your organization's credit rating may drop, making it harder to raise capital. And your company's cyberthreat insurance premium can increase significantly, even if you make substantial investments to secure your IT infrastructure and processes.

Direct and Hidden Costs of Data Breaches

Direct

- Technical investigation
- Customer breach notification
- Post-breach customer protection
- Regulatory compliance
- **Public relations**
- Attorney fees and litigations
- Cybersecurity improvements

Hidden Costs

- Insurance premium increases
- Increased cost to raise capital
- Operational disruption
- Lost value of customer relationships
- Lost contract revenue
- Devaluation of trade name
- Loss of intellectual property

CONSEQUENCES OF DATA BREACHES

Reputational Damages

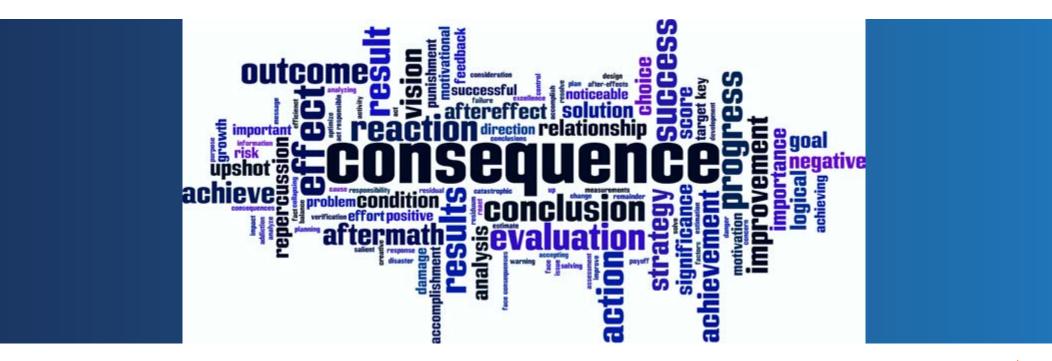
While the above financial costs may severely impact your enterprise, they can pale in comparison to your customer losses and the inability to attract new clients because they doubt your ability to protect their data. Additionally, you may find it more difficult to retain employees or find top talent in the future.

Intellectual Property Loss

Data breaches could affect your enterprise's competitive position for years to come, should proprietary information fall into the wrong hands. For example, your competitors could take advantage of your leaked blueprints and trade secrets to develop better products—and launch them before you do. Or your organization may no longer meet the conditions necessary to patent an invention, one that would have given you a long-term competitive advantage.

What About Pretending a Breach Never Happened?

Beyond being unethical and irresponsible, simply ignoring that a breach has occurred is illegal in most cases. The vast majority of countries around the globe have set (or are in the process of setting) breach notification laws that include mandatory reporting to protect individuals whose personal information might be at risk. Ignoring these laws can carry harsh civil—and criminal—penalties.



PREVENTING EMAIL DATA LOSS

In light of the severe consequences that can arise from data breaches and the associated laws addressing them, most enterprises proactively choose to invest in cybersecurity, with "protection and prevention" being their primary spending priority. When it comes to email, there are three key strategies your company should consider in order to minimize your risk of data theft and loss:

1. Authentication & Encryption

Hackers may try to attack your systems directly to access confidential data, or they can catch emails as they transit via an insecure transport link. The good news is that protocols (including DKIM, DMARC, SPF and TLS) are designed to prevent most instances of unauthorized interception, content modification and email spoofing. Encryption and authentication, however, do not safeguard you against human errors and misdeliveries.

2. Policies & Training

It is vital that your company develops and implements security guidelines and rules regarding the circulation and storage of sensitive information—as well as clear steps to follow when a security incident happens. Once you have defined these policies and procedures, you must also ensure that your employees are fully aware of them, and undergo training when they join your organization—or after every significant security update.

3. Data Loss Prevention

However, this added convenience can encourage your employees to let their guard down and forget to check whether they have selected the right person before sending a message. Disabling auto-complete and requiring your employees to type each email address manually for every message they send is one answer, but highly inefficient and frustrating to users.

Alternatively, you can choose to install an email data loss prevention (DLP) solution to prevent misdeliveries without hindering productivity within your organization.

VIPRE SafeSend: How Email DLP Works

In a nutshell, email DLP solutions like VIPRE SafeSend enable your company to implement security measures for the detection, control and prevention of risky email sending behaviors. This technology doesn't impede the working practices of your employees (unlike a policy of disabling autocomplete cache) while still minimizing the risk of accidental emailing.

Consider these fictional use case examples, and the markedly different outcomes they produce based on whether VIPRE® SafeSend® is deployed:

Example: Confirm Recipients and **Attachments**

Lara who is a product manager who interacts with a wide variety of internal stakeholders, and frequently exchanges confidential documents with colleagues in R&D, marketing and sales. She also directly supports many customers during product onboarding, training and escalations. As such Larg, sends dozens of emails every day—and due to her extensive contact lists, there's always a risk that someone unintended ends up in the TO or CC fields.

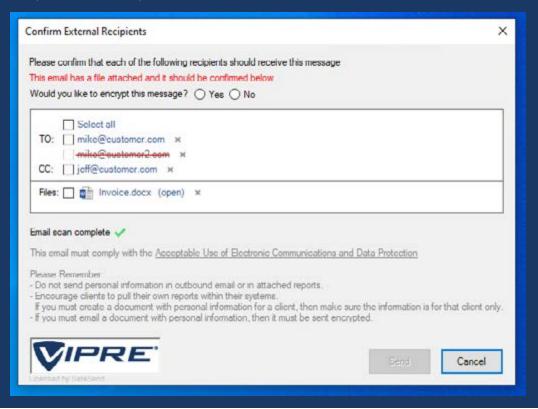
If Lara makes that mistake...

Without VIPRE SafeSend

She's in big trouble. Her email has likely been delivered already, and there's little she can do except try to recall it—with a high probability of failure.

With VIPRE SafeSend

A window would have popped up and flagged any personal, misspelled or spoofed email address that Lara selected, giving her the opportunity to go back to her email draft and remove any unwanted recipients.



VIPRE SafeSend: How Email DLP Works

Example: Advanced Content Scanning

Employees may not always remember which files contain highlysensitive information, or they can get distracted when hurriedly working. That is exactly what happened to Anna, who attached the wrong file after receiving an urgent request from Jim (an account manager) to send him some sales collateral.

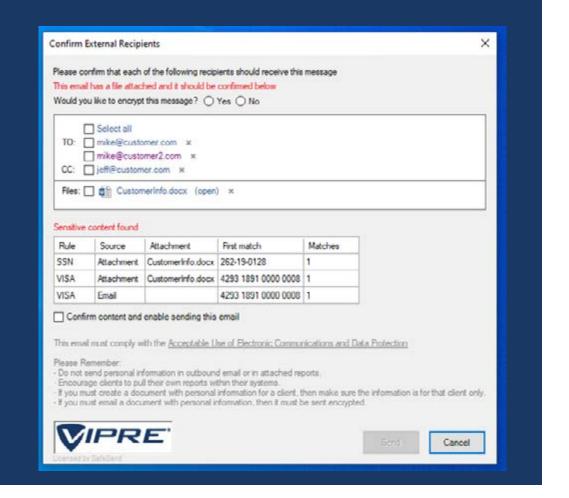
Neither Anna nor lim knows that the document she mistakenly sent contains a list with thousands of credit card numbers.

Without VIPRE SafeSend

Their company is on the verge of a massive data breach because Jim did not open the file first—and is about to send it to a multitude of potential clients.

With VIPRE SafeSend

With SafeSend's advance scanning functionality, this breach would have been prevented from the start. Anna would have seen a confirmation window like the one shown and realized the attached file was filled with credit card numbers.

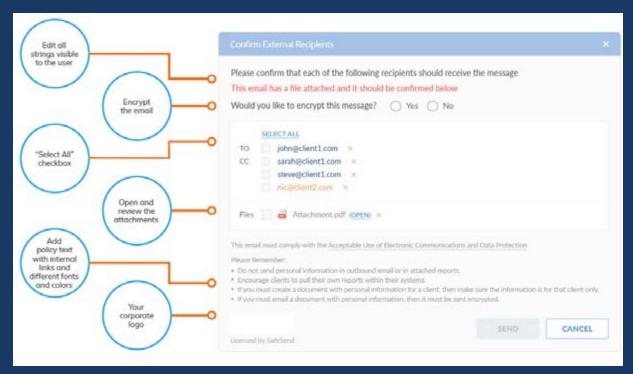


VIPRE SafeSend: How Email DLP Works

Example: Centrally-Managed Settings

To put it bluntly, how good are a company's security policies if they can't be enforced? Organizations must have the ability to consistently implement their departmental and employee-specific rules concerning data circulation if those rules are to be truly effective.

How can an enterprise be sure everyone is following its security policies?



Without VIPRE SafeSend

The company probably lacks the control required to verify compliance with its policies, and can only hope its employee training was enough to encourage best security practices in email communications.

With VIPRE SafeSend

The enterprise can easily ensure its security policies are being observed, and seamlessly manage rules and exceptions both internally and externally. This is particularly convenient if the organization wants to add an extra confirmation step only for departments and users working with commercially-sensitive information.

CHOOSING AND INSTALLING AN EMAIL DLP SOLUTION

Despite what you might think, the selection and installation of an enterprise-class email DLP solution can be remarkably simple. Below is an overview of the steps you should follow when evaluating and deploying VIPRE SafeSend (or other email DLP products):

1. Check System Requirements

First, make sure to check the email DLP solution you're considering fits with your existing IT infrastructure and systems. For example, SafeSend is compatible with all recent versions of Outlook and Windows used in today's enterprises.

2. Link Your Email User Policy

Next, ensure the email DLP solution you choose offers you enough flexibility to implement your corporate information security policy.

For example, you might need the ability to:

- Notify users when an email address seems to be added by mistake (e.g., all addresses end in "@client1.com" but one ends in "@client2. com")
- Remind users about key rules and other info before they send an email
- Set different permissions, security measures for internal/ external contacts
- Specify content scanning rules (e.g., flagging 16-digit credit card numbers)
- Notify users when their message is addressed to more than XX recipients
- Distinguish between safe, unsafe, and forbidden domains

3. Deploy Solution

Installing the email DLP solution should be as simple as possible, with the option to deploy the software either individually on each machine or all computers at once. Your IT administrator should also be able to configure and manage the security settings centrally, without requiring redeployment.

4. Inform End Users

The email DLP solution you select should be intuitive to use and promote best sending practices. For example, every SafeSend confirmation window tells users why a breach may occur if they send the email as is, and provide them with a link to your information security policy for more information if needed. (Educational material—articles, how-to guides, videos—can also help train your employees.)

5. Monitor Security Performance (optional step)

Keeping an eye on how employees are using email can help your organization strengthen its security and implement better policies. For example, SafeSend integrates with SIEM applications such as Splunk, enabling you to analyze how much sensitive information is being transmitted by your company's employees, so you can detect and remediate any bad email sending practices.

CONCLUSION

Email is the most widespread form of corporate communication, and virtually no company would be able to operate without it. But email is also a common cause of data breaches which can result in massive fines, irreparable reputational damages and costly intellectual property losses.

To combat these breaches, savvy enterprises invest heavily in email security technologies with authentication and encryption capabilities. These solutions and protocols may do an excellent job tackling intentional external threats (hacking, malware, spoofing, phishing) but offer little help when it comes to stopping inadvertent disclosure of sensitive data to the wrong recipient.

BOTTOM LINE

The risk of revealing confidential information exists in every email that's sent by your organization's employees. That's why we offer SafeSend, a powerful and user-friendly solution that enables enterprises to prevent accidental emailing without disrupting the day-to-day business practices of their employees.

SafeSend is an industry leader in the prevention of accidental emailing, and is designed to meet the needs of mid-size and large organizations by offering over 70 configurable settings, as well as a variety of API integration capabilities for email encryption, SIEM, and incident management.

Trusted by over 200,000 users around the world, SafeSend processes more than 5 million emails every day, and is compatible with Outlook and Windows. Visit https://www.vipre.com/products/business-protection/safe-send-software-outlook/ to request your free trial today.

ABOUT VIPRE

VIPRE is a leading provider of Internet security solutions purpose-built to protect businesses, solution providers, and home users from costly and malicious cyber threats. With over twenty years of industry expertise, VIPRE is one of the world's largest threat intelligence clouds, delivering unmatched protection against today's most aggressive online threats. Our robust software portfolio includes comprehensive endpoint and email security, along with threat intelligence for real-time malware analysis. VIPRE solutions deliver easy-to-use, comprehensive, layered defense through cloud-based and server security, with mobile interfaces that enable fast threat response. A proud Advanced Technology Partner of Amazon Web Services, VIPRE operates globally across North America and Europe. VIPRE® is a subsidiary of J2 Global, Inc. www.VIPRE.com

