



## Reducing Email Threats

MyMail Solves Common Privacy and Security Email Threats

MyMail Technology, LLC  
2009 West Beauregard Avenue  
San Angelo, TX 76901  
(866) 949-8572  
[www.mymail.com](http://www.mymail.com)

March 2008



# REDUCING EMAIL THREATS

---

## MyMail Solves Common Privacy and Security Email Threats

The Most Common Email Threats .....	2
MyMail's Secure Email Solution Reduces Common Email Privacy Threats.....	2
MyMail's Secure Email Solution Eliminates Eavesdropping .....	2
MyMail's Secure Email Solution Reduces Identity Theft .....	2
MyMail's Secure Email Solution Eliminates Unauthorized Message Manipulation .....	3
MyMail's Secure Email Solution Reduces (FEAR) False Emails Appearing Real .....	3
MyMail's Secure Email Solution Overcomes Lack of Evidentiary Standing.....	3
MyMail's Secure Email Solution Reduces Common Email Security Threats.....	
MyMail's Secure Email Solution Stores Email Messages Redundantly .....	3
MyMail's Solution Eliminates Inside Email Snooping and Theft.....	3
The MyMail Secure Email Solution Does Not Retain Traditional Log Files .....	4

## The Most Common Email Threats

There are several common threats that affect the personal, private and confidential nature of Email communications.

- Email Privacy Threats
  - Eavesdropping
  - Identity Theft
  - Loss of Privacy
  - Message Manipulation
  - False Emails Appearing Real
- Security Threats
  - Inside Snooping and Theft
  - Lack of Evidentiary Standing
  - Unauthorized Email Backups
  - Non-Deleted Messages
  - Log Files

## MyMail's Secure Email Solution Reduces Common Email Privacy Threats

### MyMail's Secure Email Solution Eliminates Eavesdropping

Standard Email solutions send personal, private and confidential information and Email identities (usernames and passwords) through the internet in plain English for just about anyone to read. MyMail protects your privacy by using patented and patent-pending technologies to safely secure and transport Email messages. MyMail's technology takes plain English messages and transforms them into gibberish as they travel through the internet to a server running MyMail's Secure Email solution. On the MyMail server, messages are further encrypted and securely stored using security keys known only by the proper recipient. When you use MyMail, all your communications are safe, secure, and private.

### MyMail's Secure Email Solution Reduces Identity Theft

MyMail reduces identity theft by using Secure Socket Protocol communication links, which ensures private communications by transforming Email credentials (username and password) and messages into gibberish as they travel across the internet, then further encrypting and securely storing Email messages using security keys known only by the intended Email recipient. Standard Email solutions do not provide the security to protect credentials or store Email, which makes it simple for hackers and snoopers to obtain credentials and use them to fraudulently access your Email account. Once hackers and snoopers steal your credentials they can read, download, delete and even send fraudulent Email. Further, Email messages sent through standard Email solutions can be read by just about anyone with a little computer knowledge because they travel across the Internet in plain English.

MyMail maintains privacy in three ways:

1. Only a minimal amount of information is in plain English; all other information is securely encrypted and stored using security keys. MyMail Email can only be read by someone who knows the correct username and password.
2. Hides internet protocol (IP) addresses in message headers, which protects personal private information such as the city and state where you live—information predators use to discover key personal information about you.
3. Encrypts all Email messages for storage and encrypts all messages for transmission.

You can use MyMail's WebMail interface or any Email client (such as Microsoft Outlook) to send and receive Email messages in full confidence. MyMail protects your privacy and is safe and secure.

### **MyMail's Secure Email Solution Eliminates Unauthorized Message Manipulation**

MyMail can be configured to eliminate administrative access to user's passwords, which prevents unauthorized access to mail messages and mail boxes. Further, since all Email messages are encrypted and securely stored using dynamic security keys, no message manipulation is possible. Any attempted modification of an encrypted Email message renders it unreadable since modification would result in a decrypted message of gibberish. With MyMail, the Email message sent is the Email message received.

### **MyMail's Secure Email Solution Reduces (FEAR) False Emails Appearing Real**

It is easy to construct Email messages that appear to be sent by someone else. MyMail employs several proprietary and published techniques — including Reverse DNS lookup, finger, and special credential validation — to identify and validate the sender's Email address is real and the message is sent from a legitimate Email server and host. Further, MyMail ensures all messages sent through its servers contain valid MyMail header information to assure recipients the message they receive is the messages that was sent.

### **MyMail's Secure Email Solution Overcomes Lack of Evidentiary Standing**

Because MyMail encrypts and securely stores every Email message using unique security keys specific to each user, no one else can forge or manipulate the contents of Email messages. This ensures message accuracy, which is necessary for contracts, business communications, electronic commerce, and medical-related communications.

## **MyMail's Secure Email Solution Reduces Common Email Security Threats**

### **MyMail's Secure Email Solution Stores Email Messages Redundantly**

MyMail employs RAID 5 or RAID 6 disk arrays for redundant/fault tolerant Email message storage, which eliminates the need for archiving the Secure Email message files. By default, MyMail maintains a redundant/fault tolerant copy of the Secure Email storage on each Secure Email server rather than archiving data via some asynchronous mechanism. MyMail does this for the following reasons:

1. Archived data is not synchronized with current data. As a result, Email messages you believe are deleted can reappear, causing unexpected consequences;
2. Because MyMail supports the use of POP3 Email programs such as Microsoft Outlook or Mozilla Thunderbird, individual users can download their own Email messages to their personal computer systems and manage their own Email message archives.

### **MyMail's Solution Eliminates Inside Email Snooping and Theft**

The majority of today's Email solutions allow system administrators complete access to your Email account and credentials (username and password), which allows them to read, edit and delete your Email messages without your knowledge. This unfettered access also allows system administrators to send Email messages as though they came from you. MyMail is configured to prevent unfettered access by system administrators. For instance, a system administrator cannot access your Email account by simply resetting and restoring your password.

MyMail provides several different configuration options, including password management. For security reasons, however, password management options are only configurable at system installation time. The password management configuration options allow system installers and administrators to configure their mail servers for various password management scenarios, which include:

1. The ability to allow a system administrator to set or reset individual passwords as they please;
2. The ability to reset an account password based upon a “universal” reset password;
3. The ability to prevent a system administrator to set, reset or recover user account passwords.

Options 1 and 2 provide detailed audit trails for password changes made by system administrators. Option 3 provides the ultimate security by allowing only you to change your password; thereby eliminating a system administrator’s ability to gain unauthorized access to your email messages.

If at installation time the “universal” reset password is set and enabled, the system administrators is allowed to reset a user’s Email account to the preset universal password, but they are not be able to restore the user’s password back to its original password. This prevents a system administrator from accessing your account without your knowledge. In addition, MyMail tracks password reset and reactivation (with a new password) in two ways. First, by entering the password reset or reactivation dates and times into a secure table that each user can inspect. Second, by sending email notifications to the Email account holder and their secret designees notifying them of dates and times the user’s Email account was reset and reactivated. These password and account access control mechanisms thwart threats of “inside snooping” that have cost many businesses millions of dollars.

### The MyMail Secure Email Solution Does Not Retain Traditional Log Files

Traditional log files are text files written in plain English which are used to assist in diagnosing problems and spotting potential security breaches. However, they often contain various forms of information such as IP address, email addresses, and other potentially private and confidential information. To prevent such log files from becoming security breaches themselves, MyMail does not retain any log files for more than 72 hours, and those log files it does keep for the 72-hour period are kept securely with only the minimum amount of information necessary to perform standard diagnostic functions.