iMail

All-Round Email Protection

iSign International

Email messages are generally transferred over untrusted networks- external networks that lie outside the user's secure network. When these messages lack appropriate security safeguards, they are like postcards that hackers can read, copy, and modify at any point along these paths. Follow this article to protect your emails using iSign's iMail client.

Having a secure email system is a fundamental right of every human being. iMail is just one of three solutions iSign provides within Wave to reduce users' threat vectors. An email client that protects their data from hackers is a wise choice for users. iMail is a secure email platform powered by patents for Biometric Signature, threat Detection, and Prevention. Anyone Looking for the confidentiality, availability, and integrity of the information sent via email should be aware of the threats that email systems face and understand the basic techniques for securing these systems.

iMail prevents automated phishing attempts from hackers

The most effective method for compromising a person's account has always been phishing email attempts, as 100% of people who conduct business online or involve in online transactions use email to communicate. By sending emails with attachments or creatively adding javascript programs into the email itself, hackers are able to gain access to your computer and install malicious software. "Browser Plugins," while very convenient have only exacerbated the problem. WAVE Browser and iMail are the solution to preventing phishing emails, WAVE Browser does not support "Browser Plugins", while iMail disables email javascript programs, therefore, preventing automated program activation. iMail fully verifies every script within an email to give

you a Phishing Rating so that you know if the email is suspicious or not. WAVE Mail's Patented AI automatically detects Fraudulent Emails pretending to be someone or some company you are doing business by utilizing machine learning.

Common Threats Faced by E-mail Systems

Because email is widely deployed, well understood, and used to communicate with untrusted, external users, it is frequently the target of attacks. Hackers can exploit email to access confidential information, gain control over the user's desktop, or disrupt access to information technology (IT) resources. Common threats to email systems include the following:

- **Malware:** Increasingly, attackers are taking advantage of email to deliver a variety of attacks to users through malicious software that contains viruses, Trojan horses, worms, and spyware.
- **Spam and phishing:** Unsolicited commercial email, commonly referred to as spam, refers to sending of unwanted bulk commercial email messages.
- Such messages can utilize IT resources excessively, disrupt user productivity, and distribute malware. Phishing is similar to spam, which refers to the use of malicious means to trick individuals into responding to the email and disclosing sensitive information. Compromised email systems are often the means to deliver spam messages and conduct phishing attacks using an otherwise trusted email address.
- **Social engineering:** Rather than hacking into a system, an attacker can use email to gather sensitive information from the user's server or get users to perform actions that further an attack. A typical social engineering attack is email spoofing. One person or program successfully masquerades as another by falsifying the sender's information to hide the exact origin.
- **Entities with malicious intent:** Hackers may gain unauthorized access to resources in the user's network via a successful attack on a mail server. For example, once the mail server is compromised, an attacker can retrieve user

credentials, which may grant the attacker access to other family members on the home network.

- **Unintentional acts by authorized users:** Not all security threats are intentional. Authorized users may inadvertently send proprietary or other sensitive information via email, exposing the user to embarrassment or legal action.

About iMail

iMail is the ONLY email client that protects user's emails from hackers. It comes with iSign's suite of security technology, which protects the user's account using biometric signature recognition, GEO recognition, proprietary auto-pairing, dual firewall technology, Dynamic PKI, 6-Factor Authentication, and the most robust encryption.

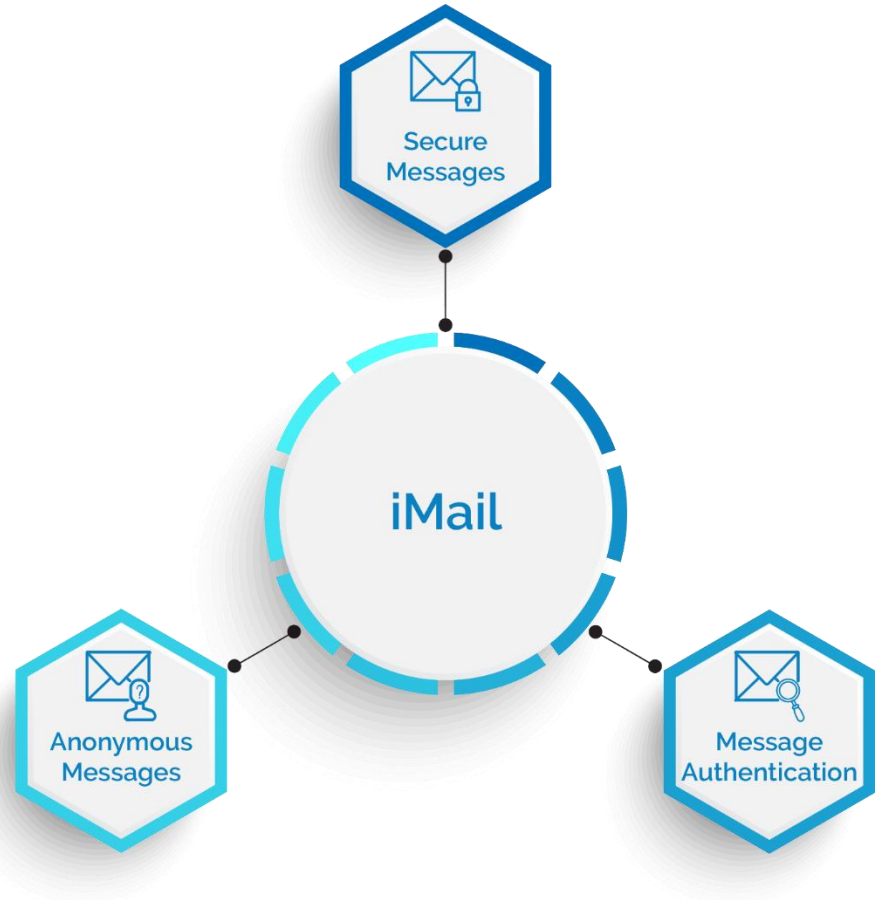
iMail is protected by 2048 Bit Dynamic Encryption while having a friendly user interface, auto group sending, email permissions, unlimited attachment sizes, high performance, and many other great features to help users stay secure and efficient.

Elements	Standard and Unsafe	Standard and Unsafe	Unified Front Triple Threat to Hackers
Web Browser	Internet Explorer / Edge	Chrome	Wave Browser
Email Client	Outlook	Gmail	iMail
Cloud Storage	OneDrive	Drive	eCloud
Unified Front Against Hacking	✗	✗	✓

iMail provides an adaptable way to communicate in a one-to-one, one-to-many, and many-to-many design. In the future, utilizing secure and encrypted communication tools will be a universal requirement.

- **Secure Messages:** iMail provides automatic end-to-end encryption from the sender to the receiver.

- **Message Authentication:** All iMail messages that lack any information about the originator are automatically signed, and the receiver checks the message's integrity and authenticity.
- **Anonymous Messages:** Email can also be delivered without any information about the originator.



Management Controls- Security Safeguards That Organizations can Implement

Management security controls like organization-wide information security policies and procedures, risk assessments, and contingency planning are essential. They ensure the effective maintenance and operation of a secure email system and the supporting network infrastructure. Additionally, we must implement and deliver security awareness and training because many attacks rely either partially or entirely on social engineering techniques on target users.

Conclusion

Securing email communication is inherent to the broader cybersecurity perspective of the user. iSign International's iMail protects user's email from the prying eyes of hackers.

To learn more about iSign and its SmartGuard innovative solution, which helps monitor and detect malicious activities in real-time by leveraging hardware-assisted security assurance for home and business environments visit our website at https://isigninternational.com/.