DATA PROTECTION 101:
What Is Email Security?

KLOUD9

TABLE OF CONTENTS

Introduction

Few forms and applications of technology have had such a profound impact on human society as email.

It revolutionized the way people communicate over long distances, the way businesses operate, and how various technologies developed. Just look at how quickly cell phones went from simply being portable phones to a typical method for sending and receiving emails.

From a business perspective, email makes it possible to send and receive everything from brief messages to important documents, allowing a level of organization and collaboration that won't be surpassed until the widespread adoption of cloud computing. Even with the advent of cloud solutions, people and organizations still rely on email.

Unfortunately, all that has made email such an integral part of our lives has also made it the primary avenue through which cyberthreats target both individuals and organizations. Whether it's with ransomware, phishing, or email account takeover, email has long been the go-to tool for cybercriminals and that is unlikely to change.

Email security is therefore vital to ensuring the safety and integrity of you and your business's systems.

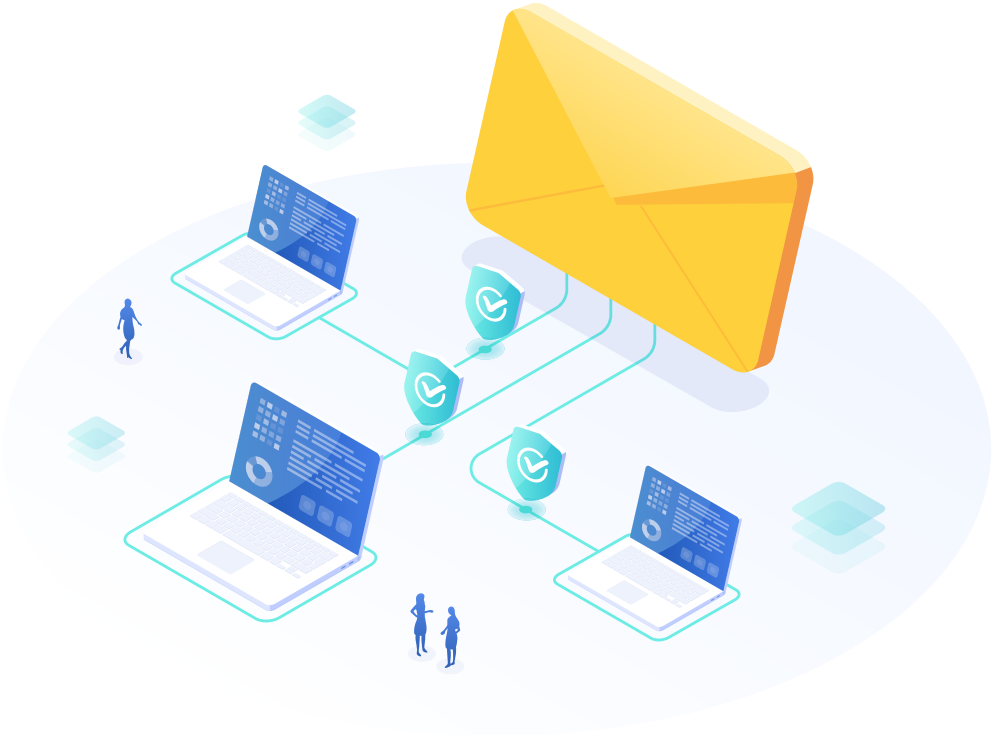
But what exactly is email security? Why is it important? What are the biggest threats to email security? How do you implement it?

Part 1- What is email security?

Email security is the combination of tools, policies, and methods that protect your email communication systems.

When properly established and utilized, email security:

- Protects the confidentiality, availability, and authenticity of your messages
- Denies unauthorized parties and programs access to your messages and accounts, preventing any resulting data breaches
- Detects and blocks malwareof protection for personal data in case the primary copy is destroyed or corrupted. Organizations should store backups in a secure off-site location that can be easily accessed in the event of an emergency.



Part 2 - Why is email security important?

The importance of of email security can be broken down into four key points:

1. Critical information

Businesses like yours are responsible for all manner of sensitive and critical information pertaining to their operations, employees, and customers. Maintaining the confidentiality of this information is vital to protecting your organization and your customers from exploitation. Any breach of that confidentiality can lead to loss of customer trust, reputational damage, and penalties and fines from regulatory bodies, all of which can result in significant financial losses.

2. Human error

An employee's email address will often be the first, second, and third vector by which cybercriminals try to target an organization and its data. Someone opening the wrong email can undo even the best, most advanced, and most comprehensive suite of cyber defenses. Cybercriminals know this and have gone to great lengths improving their methods to maximize and take advantage of the slightest slip-up.

Well-constructed and maintained email security measures mitigate the risk of data breaches caused by human error.

3. Initial cyberthreat intrusion

If they get into an employee's email account, a cybercriminal can exploit any data shared through that account. They can obtain login credentials, confidential customer information, or simply infect that employee's workstation with malware. Often enough, that's all it takes. Once cybercriminals gain entry into a system through email, it can be months before their presence is detected, by which point they may have infected countless other systems. And that's if they don't launch a ransomware attack or deploy some other threat across an organization's critical networks.

The purpose of email security is to prevent initial intrusions from occurring, which is far less costly than mitigating the damage of a full data breach or the following recovery process.

4. Ineffective standard security

Although email service providers include their own set of protections and safeguards, these are often insufficient against motivated cybercriminals. Standard email security measures are only effective against threats they already recognize, and cybercriminals are constantly developing new methods of attack. While email providers do distribute updates to protect emails from new threats, there can be a relatively long period (by digital standards) during which your emails are vulnerable.

Comprehensive security measures incorporate real-time threat detection and analysis, artificial intelligence databases, and other methods that are normally beyond what standard email security offers. Thus, individuals and organizations serious about email security must employ more advanced security measures on their own initiative.

Part 3 - The components of email security

To protect the integrity of your email platform, email security will often leverage the following tools:

1. Access management

Email security enables users to prevent unauthorized devices from accessing emails. This is especially relevant with the rise of remote and hybrid work practices, as people at home use devices that may not be secure. With access management, organizations ensure that emails and accounts can only be reached through devices and user accounts approved or provided by the company.

2. Encryption

Encryption is the process that makes data and content unreadable or inaccessible unless someone has the decryption key. Email security uses end-to-end encryption tools to maintain the confidentiality of email messages, ensuring critical and private information is protected, even if an email falls into the wrong hands.

3. Email traffic monitoring

One of the signs of a compromised system is excessive email traffic, both inbound and outbound, outside of what is necessary for business operations. Large email traffic can contain spam, bulk messages, and even cyberthreats. With the right email security tools, you can monitor this traffic, alert users, and trace the traffic back to its source if it originated within your system.

4. Threat detection and protection

Effective and up-to-date email security can recognize known phishing, ransomware, and other malware threats as they appear in your email traffic. They typically look for obvious signs of an email threat such as unfamiliar email addresses or domains, URLs, and attachments. Email threat detection software will automatically filter or remove any incoming messages containing these elements, preventing potential threats from taking root in your system.

5. Advanced tools

In addition to encryption, access management, threat detection, and various forms of anti-malware protection, email security employs a variety of cutting-edge tools to safeguard your system, such as:

- **Machine learning (ML):** As a form of AI that does not need additional programming, ML systems can analyze existing patterns of email behavior and use it to detect suspicious activity, such as emails being sent outside of office hours.
- **Sandboxing:** This cybersecurity tool creates a virtual environment cut off from the rest of your systems where suspicious emails or attachments are opened and analyzed. This allows you to test and confirm whether an unsolicited email is indeed a threat without worry of it affecting the rest of your systems.
- **Predictive analytics:** Another AI-based security tool, predictive analytics breaks down and analyzes vast swaths of data in a short amount of time. Email security can use predictive analytics to study previous cyberattacks to predict the form and methods of future attacks.

Part 4 - Email security threats

The volume and variety of cyberthreats that utilize email as an attack vector can be worrying. That's why it's important to recognize the most notable of them so you can prepare accordingly.

Phishing

Few cyberthreats are as prevalent or so closely associated with email as phishing attacks. By pretending to be from a legitimate organization or sender (and in some cases the target's own company), phishers try to convince targets to disclose private credentials or information.

The content of the phishing email may take the form of a plea for help, an appealing sale or offer, or an urgent warning that your system has been compromised. To resolve the presented crisis or offer, the phisher will bid the target to either send the "necessary" information directly via an email reply or input it on a website they control. In the case of the latter, phishers or their co-conspirators will set up elaborately disguised websites, so the target will be none the wiser as they input their bank login information or Social Security number.

Furthermore, phishing can take many forms, including:

- **Spear phishing,** which has been tailored to target an individual to increase the likelihood of success;

- **Whaling,** which is similar to spear phishing but even more specialized to target key individuals within an organization who possess access to high-value credentials and information; and
- **Vishing,** smishing, and social media phishing, which use non-email vectors, including voice calls, SMS text, and social media platforms, respectively.

Fraud

Similar to phishing, fraud is a method in which the cybercriminal pretends to be a legitimate organization or entity. Unlike phishing, wherein the aim is to obtain confidential information, the intent of fraud is to convince the accounting branch of an organization to transfer funds to an account that the fraudster controls.

Domain spoofing

Less a form of cyberattack and more a cyberattack tool, domain spoofing involves the creation of a fabricated website or email domain to make the emails of cybercriminals appear more legitimate. This makes it easier to conduct a wide range of social engineering scams and phishing attacks.

Malware

Less a form of cyberattack and more a cyberattack tool, domain spoofing involves the creation of a fabricated website or email domain to make the emails of cybercriminals appear more legitimate. This makes it easier to conduct a wide range of social engineering scams and phishing attacks.

Malware

Less a form of cyberattack and more a cyberattack tool, domain spoofing involves the creation of a fabricated website or email domain to make the emails of cybercriminals appear more legitimate. This makes it easier to conduct a wide range of social engineering scams and phishing attacks.

- **Adware** generates advertisements, often in the form of pop-ups, at a rate that is distracting and inconvenient.
- **Scareware** will attempt to scare the target, usually with a brightly colored and urgently worded pop-up that says they have a virus or some other cyberthreat. From that point, the pop-up will try to direct the target to an infected website or download more malware.
- **Spyware** is a less overt form of malware that sends data obtained from the target's systems back to the sender.

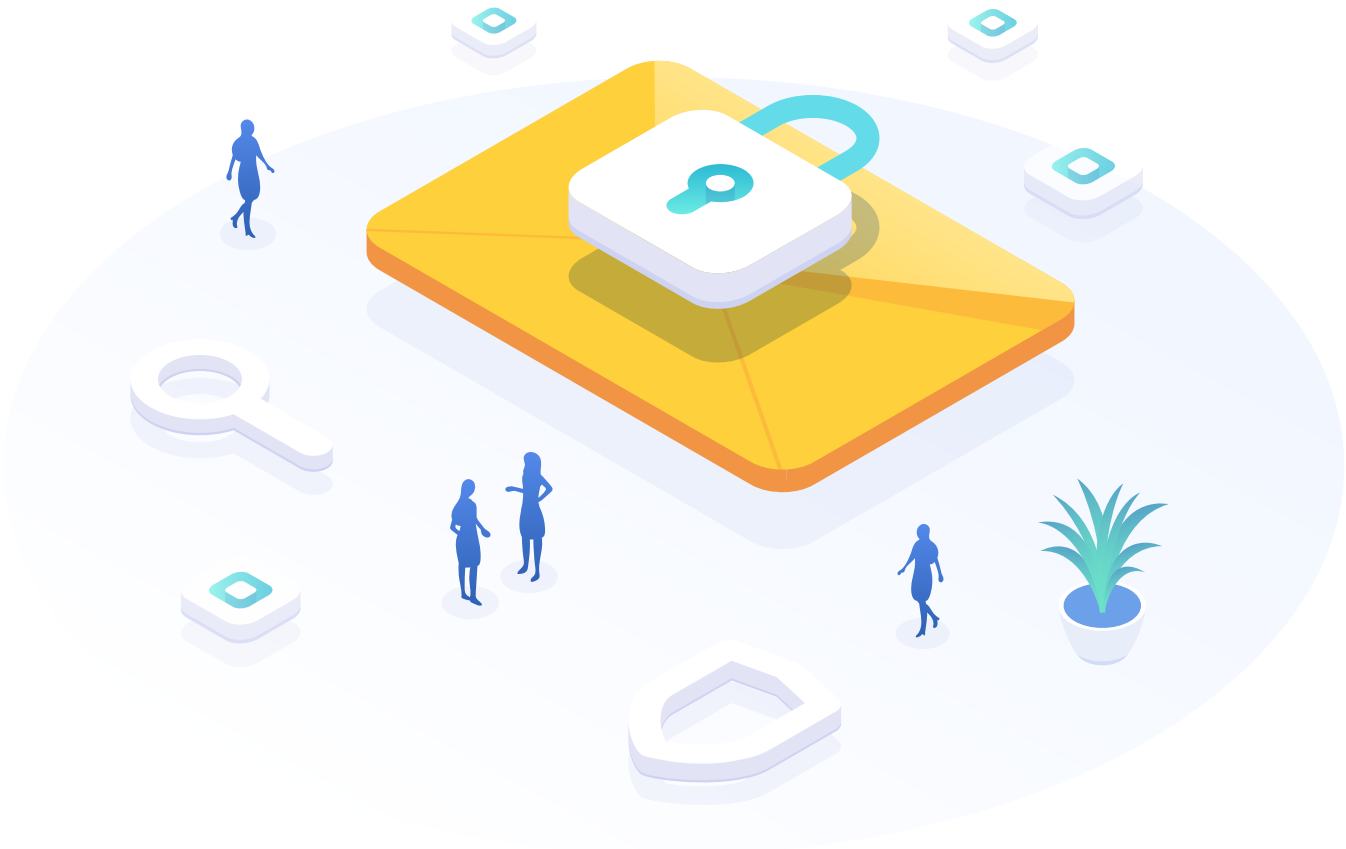
Ransomware

Among the forms of malware that can threaten an organization through email, ransomware deserves its own entry on this list. This form of malware operates by encrypting a target's critical data, making it inaccessible to the target. The only way to restore the data is with a decryption key that the ransomers will only provide in return for a sizable payment, usually in an untraceable cryptocurrency such as Bitcoin.

Even if a target refuses to pay and manages to restore the encrypted data from a data backup, the recovery costs and regulatory fines can still be high. An unsuccessful ransomware attack will still bring an entire organization and its operations to a halt, then force it into a recovery phase that can last for months. To make matters worse, cybercriminals are developing new forms of ransomware, such as ransomware 2.0, which creates copies of the encrypted data, giving hackers a vise grip on their victims even when they've already paid the initial ransom.

Email account takeover

While other forms of cyberattack discussed in this eBook use email as an attack vector, email account takeover targets the email system itself. Cybercriminals can use various methods to take control of a target's email account, such as password guessing, spyware, keyloggers, and brute force attacks. From there, they can obtain information, spy on emails, and even use the stolen account as a launching point for malware, phishing attacks, and fraud (possibly even on the target's own company).



Part 5 - Email security policies and best practices

Effective email security is not a passive system. To take full advantage of it, you need to incorporate best practices and policies that make full use of the resources at your disposal, which include more than advanced software and technology.

Educate employees

One of the most important and overlooked email security measures is employee education. By training employees, an organization can teach them to recognize phishing attempts, create stronger passwords and manage them with care, and react properly in response to cyberattacks. For optimal results, it's crucial to conduct training regularly and implement simulated phishing attacks to prepare employees for real-world scenarios.

Maintain data backups and recovery protocols

No cybersecurity setup is completely impenetrable. As such, organizations need to prepare in case of a successful data breach by creating extensive data backups and having a disaster recovery process in place. This setup preserves the data in a worst-case scenario and ensures a faster, less costly restoration of regular business activities.

Implement extensive authentication

Much of email security revolves around authentication, whether that means ensuring a sender is legitimate or that only authorized personnel can access email accounts.

To verify that an email comes from a legitimate sender or prove to others your emails are authentic, check for and implement any of the following methods:

- ☐ Sender Policy Framework (SPF)
- ☐ DomainKeys Identified Mail (DKIM)
- ☐ Domain-based Message Authentication, Reporting and Conformance (DMARC)

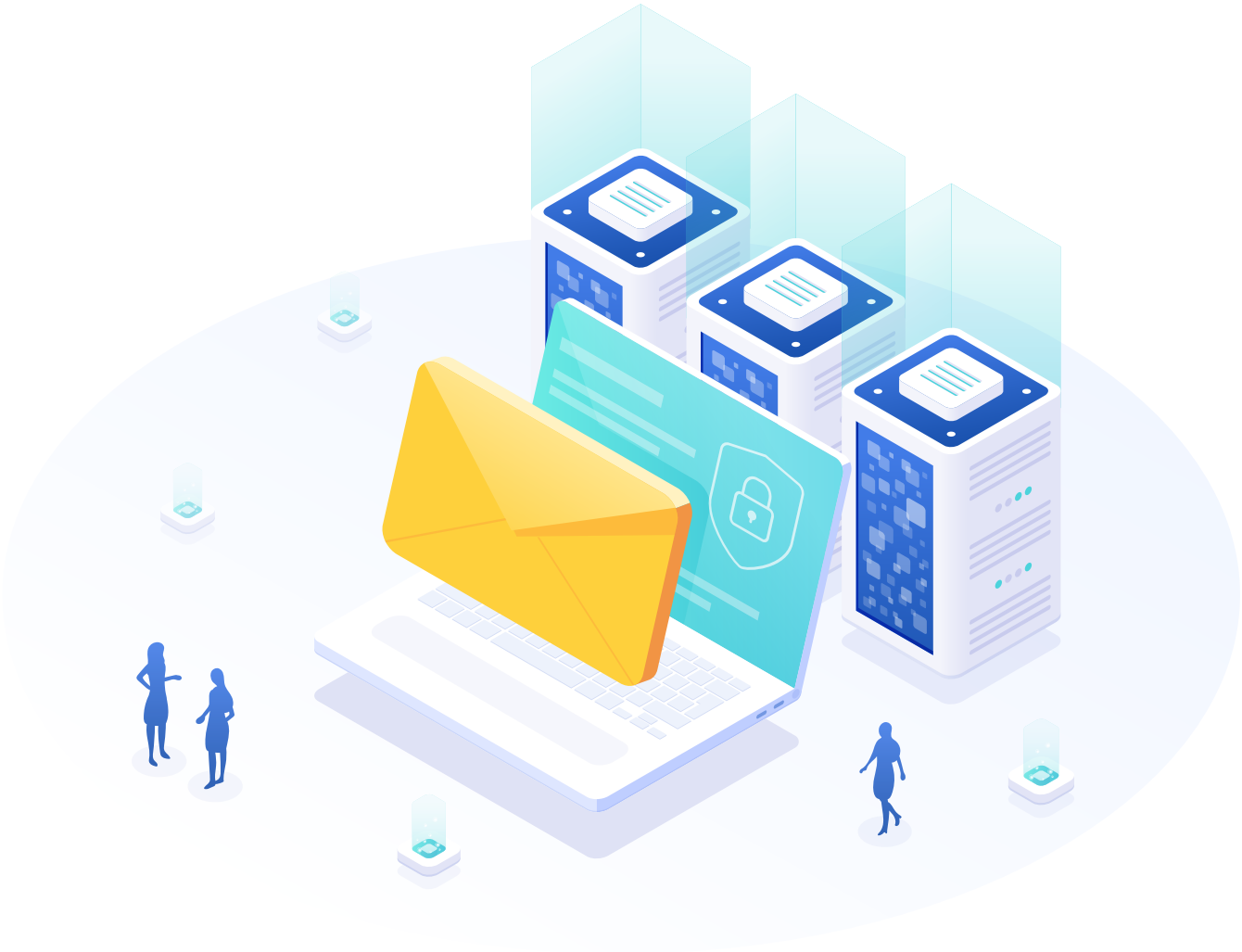
To protect your organization's email accounts and further ensure that only authorized personnel can use them, consider incorporating multifactor authentication (MFA). This authentication tool sends a one-time passcode to a secondary device or account that only the intended employee can access. That way, even if a cybercriminal somehow obtains an employee's login credentials, they cannot receive the generated passcode to access the email account.

Use a secure email gateway (SEG)

SEGs use machine learning and other tools to analyze emails mid-transit, identifying and blocking malicious email in both inbound and outbound traffic. This prevents the likes of phishing emails from even appearing in user inboxes, minimizing instances of human error.

Partner with a security provider

Constructing, implementing, and maintaining comprehensive email security requires a great deal of resources and attention. In addition, it necessitates a level of expertise and knowledge that may be beyond the scope of most organizations. By partnering with a security provider, your organization gets all the benefits of email security — including skill, tools, and solutions — without the extensive resource cost.



Conclusion

Ensuring your email is secure demands a multilayered and multipronged approach that uses technology and policy working in concert to achieve the best results. By being thorough and diligent, you can safeguard the integrity of your emails for you and your business.

Are you ready to protect your data with email security?
Contact us today to get started.

Phone: **844- KLOUD9IT (5568394)** Email: **info@kloud9it.com**