Communications Security Establishment Canada

Centre de la sécurité des télécommunications Canada

CANADIAN CENTRE FOR CYBER SECURITY

Email security best practices

Management

Foreword

This is an UNCLASSIFIED publication that has been issued under the authority of the Head of the Canadian Centre for Cyber Security (Cyber Centre). For more information, contact us by phone at (613) 949-7048 or 1-833-CYBER-88 or by email at contact@cyber.gc.ca.

Effective date

This publication takes effect on August 21, 2025.

Revision history

Revision	Amendments	Date
1	First release.	August 21, 2025

D97-4/60-002-2025E-PDF
ISBN 978-0-660-78520-2

Overview

In today's digital landscape, it is vital for your organization to protect sensitive data. Although email is a fundamental means of communication, it is susceptible to various threats. Email serves as a primary channel for exchanging information which means your organization must implement strong security measures to protect data. This publication provides guidance on the key email security practices and protocols your organization should adopt, with the goal of strengthening your defences and upholding the confidentiality, integrity, and availability of your communications and data. This publication will assist your organization in implementing protective measures such as encryption, authentication, and secure gateways. In addition to protective measures, you should also enhance your employees' awareness of and compliance with cyber security requirements and best practices. Collectively, these measures will enhance your organization's confidence to navigate the digital landscape, all while ensuring the security and privacy of your sensitive information.

Table of contents

1 Introduction

Email serves as an important communication tool for individuals and organizations and is widely used on various devices. In organizational information technology (IT) operations, email is particularly important for internal and external business communications. Its extensive use makes it a prime target for threat actors aiming to exploit vulnerabilities and compromise sensitive data. Notably, email was not initially designed with security and privacy in mind. The technologies used today that enhance email security, such as encryption and authentication protocols, were added later to help mitigate the risks associated with email communications.

With threat actors constantly refining tactics to exploit email vulnerabilities, establishing a strong defence through comprehensive email security measures helps safeguard the confidentiality, privacy, and integrity of your digital communications. Email accounts house a large amount of private information, including personal data, financial details, and confidential business exchanges. Ensuring secure email communications is important to prevent breaches that could compromise the integrity of these exchanges. Email security also protects against malware and phishing attacks, which are frequently initiated via deceptive emails. Additionally, ensuring the availability of email systems is an important aspect of email security. This helps prevent disruptions, downtime, and potential data loss that could occur from attacks on vulnerable systems.

For many organizations and businesses, adhering to industry regulations and compliance standards is essential to avoid legal repercussions and to safeguard reputation. By establishing strong email security measures, you can demonstrate compliance and assure customers/clients and partners that the confidentiality, integrity and availability of their sensitive information is handled correctly.

1.1 Common email threats

While email is a widely used communication tool, it comes with risks. Email threats are diverse, evolve constantly, and can range from deceptive phishing schemes to harmful malware. In this section, we will explore some of the most prevalent threats that can compromise your organization's private information and digital security.

1.1.1 Phishing

An email phishing attack is a deceptive tactic employed by threat actors who send seemingly legitimate emails to users. It stands out as the most common threat to email security. Although it used to be relatively easy to spot phishing attacks, they have become more sophisticated over time. Due to the advent of artificial intelligence (AI), email content no longer contains poor spelling or common tropes or lures but are now well-crafted messages containing seemingly legitimate content making harder for the reader to detect.

Phishing attacks can be generic or targeted. In the case of targeted attacks, also known as spear phishing, threat actors conduct thorough research to craft well-designed emails aimed at specific individuals or groups with special privileges or access to valuable information.

Whaling, a specific form of spear phishing, is directed at high-ranking individuals within an organization, with threat actors posing as trusted authorities. The main goal remains consistent: manipulating users into disclosing sensitive information, such as usernames, passwords, and bank account details. Threat actors may also try to get users to click on malicious links, open harmful attachments within the email, or instruct them to make unauthorized changes within a system they have access to. It is essential for you to stay vigilant and understand how phishing attacks evolve to protect your organization from such threats.

For more information on phishing attacks and malicious email and how you can avoid, identify, and handle them, read our publications:

- Don't take the bait: Recognize and avoid phishing attacks (ITSAP.00.101)
- Spotting malicious email messages (ITSAP.00.100)

1.1.2 Spoofing

Email spoofing is a deceptive tactic in which threat actors manipulate the sender's details in an email header, making it look like the email is from a trusted source. The primary objective is to trick recipients into believing the email is legitimate and to entice them to open it and engage with its contents.

The inherent danger is that spoofed emails usually contain malware or viruses, as well as malicious links that point to spoofed websites or services. Simply opening the email can expose the recipient's device to potential threats, making it vulnerable to further exploitation. Spoofing is commonly employed in both phishing attacks and business email compromise (BEC) scams. The ramifications of falling victim to such attacks extend beyond immediate harm. If sensitive information is disclosed in response to a spoofed email, it can result in identity theft.

To mitigate the risks associated with email spoofing, get in the habit of always hovering over links in an email before clicking to verify the actual URL, ensuring it matches the expected domain and appears legitimate. Avoid clicking on links that look suspicious or unfamiliar. Always consult with your organization’s IT security department if you have concerns. You should also scrutinize any email that contains unusual requests, such as urgent financial transactions or demands for sensitive information. It is prudent to verify these requests through other communication channels, like a phone call to the sender or manually visiting the website in your browser to confirm the email's claims.

Another important consideration is the potential for homograph attacks, where malicious actors use characters from other alphabets, such as Cyrillic or Greek, that look like Roman letters to create deceptive email addresses or URLs. Pay close attention to subtle differences in characters that might indicate a spoofing attempt. By combining these strategies, you can better protect yourselves from the risks of email spoofing.

1.1.3 Malware

Threat actors often use email to deliver several types of malware, such as viruses, worms, ransomware, and spyware. Malware can be directly attached to emails or embedded in shared documents sent as attachments, links, or through cloud-based storage. Once malware infiltrates a user's device, it can potentially gain unauthorized access to system components, compromise or steal sensitive information, and encrypt files. For information on how to defend against and recover from ransomware, read our publication Ransomware playbook (ITSM.00.099).

1.1.4 Business email compromise

BEC presents a growing concern for organizations of all sizes and across various industries. This sophisticated scheme often targets businesses engaged in wire transfers. Threat actors aim to defraud organizations by posing as executives or business partners to trick employees into transferring funds to fraudulent accounts.

These intricately planned and precisely directed attacks involve significant amounts of money, which makes them one of the most financially damaging threats to email security. While BEC scammers may exploit and steal data, their primary goal is financial gain, and they focus on deceiving organizations through social engineering tactics like impersonation. For more information on how to protect your organization against social engineering, read our publication Social engineering (ITSAP.00.166).

1.1.5 Impersonation

Impersonation is used by threat actors to exploit trust, benefit financially, or access sensitive information through email. For instance, in BEC, threat actors pose as trusted individuals, like employees, to steal from companies or their clients and partners. Another example is an attorney impersonation attack, where the attackers pretend to be legal representatives and often target employees who may lack the knowledge or authority to verify the legitimacy of the attackers request. Similarly, threat actors have been known to impersonate authorities, including regulators, government departments, and law enforcement agencies.

Another tactic is brand impersonation, where threat actors falsely associate themselves with well-known brands to trick recipients into revealing confidential information. There are many different impersonation techniques, ranging from mimicking internal personnel to committing financial fraud to leveraging the credibility of reputable brands for illicit purposes highlighting the need for vigilant email security practices.

1.1.6 Data exfiltration

Data exfiltration involves the unauthorized transfer or removal of sensitive information from an organization's email system. Threat actors use various techniques, such as phishing, spyware, or malware, to exfiltrate data. This exposes organizations to potential cybercrimes, including extortion and the illicit sale of data on the dark web. In turn, this can have significant business consequences, including costly data breaches and legal repercussions. To learn more on how to protect your data from exfiltration, read our publication Defending against data exfiltration threats (ITSM.40.110).

1.1.7 Spam

Businesses frequently employ spam (unsolicited messaging) as a means of promoting their goods, services, or websites for commercial purposes. Although spam may not be considered as severe as certain other email security threats, spam emails do carry inherent security risks. Email providers generally identify and filter out such messages, but spam is still a potential threat, as some emails that contain malicious links or attachments may be missed by the email provider filter.

2 Email security protocols

Email security protocols are important for protecting digital communications, as they prevent unauthorized access to email content. These protocols establish rules and standards that govern the transmission, reception, and handling of email messages between servers and clients. By defining precise steps and rules for sending, receiving, storing, and retrieving emails, protocols help establish a secure email communication process.

This section provides an overview of several established email security protocols that enhance email security. By integrating these email security protocols and practices, you can create a comprehensive and layered defence against many threats and ensure the confidentiality, integrity, and availability of your email communications. The Cyber Centre's publication Implementation guidance: email domain protection (ITSP.40.065 v1.1) provides guidance on implementing technical security measures to protect your organization's domains from email spoofing.

2.1 Transport layer security

Transport layer security (TLS), which replaces secure sockets layer (SSL), is a cryptographic protocol for establishing a secure communication channel via a 'handshake'. During a TLS handshake, the two communicating sides, typically a client and a server, exchange cryptographic keys and encrypt subsequent data transmissions. While SSL protocols and older versions of TLS are considered insecure, the latest TLS protocol version ensures email remains confidential during transit. This means that as an email travels across the Internet, it is encrypted and protected from eavesdropping. However, while the email may be encrypted during transmission, the sending and receiving servers can still access the plaintext message. Therefore, TLS does not offer end-to-end confidentiality.

Additionally, email transmitted over the Internet typically undergoes multiple intermediary transfers across various servers before reaching its destination. While TLS can secure the initial transfer from the email client to the first server, there is no guarantee that subsequent transfers will employ TLS encryption. Consequently, you should not rely solely on TLS to protect sensitive information unless you trust the receiving infrastructure and the organization operating the email servers. This is particularly important when considering the difference between securing communication between an email client application and a server and achieving end-to-end confidentiality between 2 individuals—the sender and the recipient of the email.

For information on how to configure TLS, read our publication Guidance on securely configuring network protocols (ITSP.40.062).

2.2 Secure/multipurpose Internet mail extensions

Secure/multipurpose Internet mail extensions (S/MIME) is a protocol designed to ensure the security of email communication through an end-to-end encryption framework. This protocol leverages public key infrastructure (PKI) with asymmetric cryptography, which involves a pair of mathematically related keys: a public key and a private key. These keys work collaboratively to establish a secure channel for communication.

S/MIME serves a dual purpose of digitally signing and encrypting messages sent over the Internet. Digital signatures authenticate the identity of the sender, while encryption ensures the confidentiality of the email content. In the encryption process, the recipient's public key is used, and successful decryption requires the corresponding private key held exclusively by the intended recipient. This ensures that the designated recipient can only access sensitive data, provided the private key remains secure. During authentication, a signature is generated using the sender’s private key and can be verified using the corresponding public key. This allows the recipient to check that the source of the message is authentic.

One of the primary advantages of S/MIME is its resilience against malicious activities such as sender impersonation and message interception. S/MIME establishes a secure framework for sending and receiving messages by requiring email clients to possess a digital certificate to authenticate the identity of the sender and encrypt emails during transmission.

While S/MIME improves email security, it is important to know that email headers remain unencrypted. This means that threat actors could access certain information about the sender and recipient. The Cyber Centre’s publication Guidance on securely configuring network protocols (ITSP.40.062) provides guidance on configuring both TLS and S/MIME.

2.3 Pretty good privacy and open pretty good privacy

Pretty good privacy (PGP), including open-source pretty good privacy (OpenPGP), ensures end-to-end encryption for secure plaintext, emails, and files, restricting access to only the intended recipient. It uses digital signatures to verify sender authenticity and relies on public-key cryptography and key management for secure communication. The cost of implementing PGP is relatively low and there are many free and open-source PGP software solutions available.

However, it should be noted that PGP requires both the sender and receiver to have compatible software capable of encrypting and decrypting messages for the encryption to work effectively. Additionally, both parties need to exchange and possess each other's public keys. Older emails that were not originally encrypted with PGP software remain unencrypted unless they are re-sent using the secure encryption process.

Popular email services such as Gmail, Outlook, and Yahoo do not natively support PGP without additional browser add-ons or supplementary software. This limitation can complicate the seamless integration of PGP into everyday email usage for many users.

Overall, PGP remains a versatile and cost-effective choice for individuals and small businesses seeking email encryption capabilities, provided they navigate its implementation and compatibility requirements effectively.

2.3.1 Secure/multipurpose Internet mail extensions versus pretty good privacy

S/MIME and PGP are virtually identical mechanisms in terms of what is done to the email message for transport. The main difference is that S/MIME uses PKI, with an emphasis on the "I" (infrastructure). S/MIME requires all users, senders, and recipients to possess certificates issued by a trusted authority or a delegate, which allows users' identities to be traced back to the authority of the certificate issuer. Certificates in S/MIME are typically distributed and updated through automated lookup in a corporate directory and require supporting infrastructure.

In contrast, PGP employs self-generated public/private key pairs that must be manually managed and maintained, as well as trust relationships that usually need to be personally verified. For example, one might request another's PGP public key and reciprocate by providing their own. However, this exchange could be vulnerable to adversary-in-the-middle (AITM) attacks or spoofing, as it occurs before a trust relationship has been established and before both parties have exchanged keys to message each other.

Data at rest is another key aspect of email security for both S/MIME and PGP. TLS-protected emails are encrypted only during transport. Once a message reaches its destination, it is decrypted and stored as plaintext on the recipient's system. This means that if someone gains access to your phone, laptop, or server, they can read all the stored messages. However, if the messages were encrypted with S/MIME or PGP, they remain encrypted even in storage unless the user opts to decrypt and store them in plaintext.

It is recommended that enterprises and organizations use S/MIME because it enables them to centrally manage accounts. For example, if an employee leaves, you can simply revoke their PKI credentials. In contrast, with PGP, you would have to inform all your employees that the employee no longer works there and that they should no longer trust their PGP credentials as there is no way for anyone other than the individual to revoke those keys. Additionally, S/MIME allows for security investigations, if required. Organizations can maintain a record of communications exchanged via S/MIME, including timestamps and sender/receiver information, which can be important for forensic analysis in security investigations. Furthermore, S/MIME allows administrators to enforce policies related to message retention and archiving, ensuring compliance with regulatory requirements, and facilitating audits or investigations into potential security breaches or misconduct. By leveraging S/MIME for email encryption and digital signatures, organizations and businesses can better monitor and investigate suspicious activities, thereby strengthening their overall security posture and regulatory compliance efforts.

2.4 Sender Policy Framework

Sender Policy Framework (SPF) is a system that uses features of domain name system (DNS) and allows domain owners to specify which servers are authorized to send emails on behalf of their domain. If you receive an email from an IP address that is not specifically permitted by the SPF record, it is likely not legitimate. When an email is sent, the recipient's mail server checks the SPF record of the sender's domain to see if the sending mail server is on the authorized list.

If the sending mail server is included in the SPF record (a "pass"), the email is considered legitimate and is usually delivered. However, if the sending mail server is not listed in the SPF record (a "fail"), the recipient's mail server may handle the email cautiously—possibly rejecting it or marking it as spam.

To effectively manage SPF policies within an organization, it is recommended to start with a softfail (~all) policy during initial testing. This allows administrators to monitor and correct any potential misconfigurations before fully enforcing a hardfail (-all) policy, which unequivocally rejects emails from unauthorized servers. Additionally, it is important to set non-mail-enabled domains and subdomains to hardfail (-all) for all emails, ensuring comprehensive protection against spoofing attempts across all aspects of the organization's digital presence.

2.5 DomainKeys identified mail

DomainKeys identified mail (DKIM) is an email authentication protocol that enhances the security of email messages by allowing the sender to digitally sign them. In the DKIM process, the email server generates a digital signature using the private key, exclusive to the domain owner, and embeds it in the message header. The recipient's server then verifies the signature using the sender's public key retrieved from DNS records, thereby confirming the integrity of both the sender and the message content. Specifically, a hash computation is performed and compared to ensure the authenticity of the message and sender. Once this verification process confirms the sender's identity and the message's integrity, the email is then delivered to the recipient's inbox.

DKIM ensures the integrity of email communication, making sure that emails have not been tampered with. It allows recipient servers to check the message's authenticity and to confirm it originates from the claimed domain. This helps prevent spoofing and impersonation attempts.

2.6 Domain-based message authentication, reporting, and conformance

Domain-based message authentication, reporting, and conformance (DMARC) helps prevent email phishing and domain spoofing by allowing domain owners to define protocols for handling unauthorized or suspicious messages. It builds on DKIM and SPF to ensure emails are authenticated before transmission, guaranteeing that they originated from the intended domain, and are sent to legitimate recipients.

A key feature of DMARC is that it lets domain owners establish policies for recipient servers. In turn, this allows messages to be handled effectively, even if they come from untrusted sources. This protocol guides the server on what actions to take when messages fail SPF and/or DKIM checks, for example, reject, quarantine, or accept. Some large email providers, such as Gmail and Microsoft, have implemented strict DMARC policies for inbound emails. They require that both SPF and DKIM authentication checks pass for emails sent from domains that have published DMARC policies with a reject or quarantine action. Specifically, for Google, this applies if 5,000 or more messages are sent per domain. Yahoo, on the other hand, requires both SPF and DKIM to pass regardless of the volume of messages sent. This policy ensures that emails from domains that fail both authentication checks may be rejected or quarantined by these email providers.

Unlike some other solutions that rely on a single point of failure, DMARC uses a resilient strategy that covers both the source and target sides of email communication. It conducts a comprehensive security check on sender information, recipient details, subject lines, body text, and other message characteristics.

Just like SPF and DKIM, DMARC is optional and requires support from both the sending and receiving sides to effectively mitigate spoofing risks. These protocols do not provide additional cryptographic protection but ensure message integrity and the authenticity of the sender.

3 Protecting your email

It is important for all organizations to secure email since this is essential for protecting sensitive data, including financial information and personally identifiable information. By adopting the recommended best practices listed in this publication and investing in email security tools (and, if needed, third-party email security services), you can strengthen your organization's overall data privacy strategy, its security, and its resilience.

3.1 Email security best practices

It is important to implement robust strategies to safeguard your emails and prevent sensitive information from falling into the wrong hands. This section explores essential best practices aimed at enhancing your email security posture, thereby instilling confidence in your email communications.

3.1.1 Use email encryption and encrypted connections

Email encryption and encrypted connections play important roles in ensuring robust email security. Together, they safeguard sensitive information throughout the communication process. Email encryption ensures the confidentiality of email content, preventing unauthorized access even if it is intercepted during transmission. It is particularly important to encrypt email when you are transmitting sensitive or confidential information, such as financial details, legal documents, or personal data.

TLS is used for server-to-client transport encryption and only provides security if you trust the email service provider. For instance, when using a public email service provider, such as Outlook or Gmail, TLS will protect the email as it transits the Internet, but the service provider can access all emails once they reach its servers. In contrast, S/MIME and PGP offer end-to-end encryption, ensuring email content remains encrypted even on the server, providing an additional layer of security. These emails can only be read when a recipient downloads them onto their device and enters their decryption key or PKI credential. It is essential to recognize that S/MIME and PGP provide the added benefit of securing emails from potential access by the email service provider. In contrast, TLS encryption only protects emails during transit.

Depending on the organization's business structure, it may be more appropriate to use a web portal protected with TLS/HTTPS to send and receive sensitive information. This approach can provide a more user-friendly method to securely transfer important documents, rather than relying on end-users to understand and consistently apply PGP or S/MIME encryption. In such systems, the data stored at-rest should be encrypted, ensuring security throughout its lifecycle. This hybrid approach leverages TLS encryption for secure transmission over the Internet and back-end encryption for secure storage, balancing ease of use with strong security measures.

3.1.2 Implement protocols to validate user identity and server identity

Implement protocols such as S/MIME and PGP to validate user identity and ensure that the sender is indeed who they claim to be. S/MIME and PGP offer multipurpose mechanisms for validating user identity, protecting against malicious infrastructure, and ensuring email content confidentiality. S/MIME relies on trust in certificate authorities (CAs) for automatic certificate management, while PGP relies on direct trust relationships. Both methods encrypt and sign email content, preventing tampering. Encrypted emails are decrypted only by the recipient's private key, ensuring email integrity.

You should also implement server identity validation (see sections 3.4, 3.5, and 3.6 for more information) in your email systems, using robust methods beyond relying solely on email addresses or IP addresses, as both are easily spoofed. SPF, DKIM, and DMARC are essential protocols that enhance email security by verifying the authenticity of the sending server, ensuring the integrity of the email content, and providing policies for handling messages that fail authentication checks.

3.1.3 Secure the email gateway

Email security gateways serve as inspection points to scrutinize and filter out malware, spam, and phishing attempts. These gateways are essential email security tools and can be deployed in various forms, such as hardware appliances, virtual instances, or cloud-based services. They operate as protective barriers between an organization's email server and the external email environment, actively inspecting incoming and outgoing emails. By effectively filtering threats like malware and ransomware, these gateways boost overall email security. The deployment flexibility of these gateways makes them adaptable to diverse organizational needs and environments.

When deploying a secure email gateway, you should consider the reliability and trustworthiness of third-party vendors. You might leverage the expertise and infrastructure of external providers who specialize in email security. These vendors typically offer 2 deployment models for spam filtering and email security: hybrid and full-cloud approaches. You should evaluate which model best suits your operational needs and security requirements.

3.1.4 Create an email security policy

An email security policy serves as a comprehensive guide for managing email communications within your organization. It covers protocols for email usage, data storage, device access, and handling email security threats. These protocols are all aimed at protecting sensitive information and ensuring the integrity of communication channels. Operating as a strategic framework, the policy does not just regulate email practices; it actively promotes a culture of cyber security awareness within the organization. By securing sensitive data and strengthening communication channels, the policy plays a pivotal role in building a resilient defence against cyber threats.

3.1.5 Monitor email activities

Organizations should implement monitoring tools to track email activity and detect unusual patterns or suspicious behavior. Regular monitoring is essential in maintaining the security of email systems, as it helps identify potential signs of a security breach. By consistently observing the activities within an email environment, organizations can detect any unusual patterns or behaviours that may indicate a compromise.

One effective approach to enhancing email monitoring is to use security information and event management (SIEM) systems. SIEMs aggregate and analyze data from various sources, providing real-time insights and alerts for any suspicious activities. By leveraging SIEMs, you can quickly identify and respond to potential threats, minimizing the risk of a successful attack.

Another important aspect of email security monitoring is reviewing DMARC reports. By regularly reviewing DMARC reports, you can gain insights into how your email domain is being used and whether any malicious activities are occurring. These reports provide valuable information about the sources of emails claiming to be from your domain and can highlight any unauthorized senders attempting to spoof it.

3.1.6 Conduct regular email security audits and testing

Regular email security audits are essential for evaluating and addressing vulnerabilities in email security solutions and for maintaining resilience to cyber threats. This involves periodic reviews to identify weaknesses and implement necessary improvements and updates to enhance overall email security measures. This allows organizations to make prompt and proactive adjustments to maintain a secure email environment.

3.1.7 Keep business and personal emails separate

Keeping personal and professional email accounts separate helps protect sensitive business information. Using work email addresses for personal matters can expose an organization to security risks and potentially compromise confidential data. Similarly, using personal email addresses for work-related communications can pose security risks to your organization, as it may violate organizational policies and circumvent standard security measures.

To mitigate these risks effectively, organizations should enforce clear policies. These policies should prohibit the use of business email accounts for personal matters and the use of personal email accounts for business activities. It is crucial to communicate these guidelines to all employees to ensure understanding and compliance.

3.1.8 Verify email links before you click on them

You should be very careful before you click on any email links or download any attachments, especially if they come from unfamiliar or suspicious sources. Take time to verify the legitimacy of links and assess the credibility of the sender by confirming that the domain name is correct or hovering over the link to see the actual address. This simple yet vital step can help you avoid falling prey to phishing scams or malware attacks and protect your personal and your organization’s information from potential security risks.

3.1.9 Block spam and unwanted senders

Blocking spam and unwanted senders is an email security practice that will help mitigate the risks associated with phishing attempts, malware distribution, and other malicious activities. You can enhance your defences by using advanced email filtering tools that analyze content and sender behavior. Update these filters regularly to ensure they are equipped with the latest threat intelligence so that they can block new spam techniques. Customize your security settings by using allow lists and deny lists, which allow trusted emails and automatically block messages from senders on deny lists. Additionally, educate your employees on identifying common spam characteristics. You should also review your blocked emails regularly to identify false positives and report suspicious emails for further investigation.

3.2 Email infrastructure security recommendations

The following sections provide guidance on security recommendations for your email infrastructure.

3.2.1 Email servers

Ensure email servers are configured according to security best practices, including disabling unnecessary services, using strong encryption for communication channels, and regularly applying security patches. You should also implement robust access controls to restrict who can manage and access the email server. Use multi-factor authentication (MFA) for administrative access.

3.2.2 Database/storage security

Encrypt sensitive data at rest using strong encryption algorithms to protect it from unauthorized access. Apply strict access controls to the email database/storage, limiting access to authorized personnel only. Regularly review and update access permissions. Implement regular backups of email data and ensure backups are securely stored and encrypted. Test backup restoration procedures periodically.

3.2.3 Physical controls

Secure physical access to servers hosting email infrastructure. Use access control mechanisms such as biometric scanners, security badges, and surveillance systems. Maintain optimal environmental conditions (for example, temperature, humidity) to ensure server reliability and longevity and ensure those systems are also appropriately secured.

3.2.4 Cloud environment considerations

When considering a cloud environment for your email services, it is essential to prioritize security measures to protect sensitive information effectively. Start by verifying that your chosen cloud-based email service provider adheres to industry-standard security practices. Review their certifications, such as SOC 2 and ISO 27001, and thoroughly examine their data protection policies to ensure they meet your organization's security standards.

Ensure that all data transmitted to and stored in the cloud is encrypted both in transit and at rest. Understand how encryption keys are managed by the cloud provider and ensure they are adequately protected to prevent unauthorized access.

Utilize the access management tools provided by the cloud service to enforce least-privilege access principles. Implement MFA for administrative accounts to add an extra layer of security.

Regularly audit your cloud environment to ensure compliance with your organization’s security policies and regulatory requirements. Monitor for any changes or incidents that could potentially impact the security of your email data.

3.3 Additional cyber security best practices to enhance email protection

While email security measures are vital, strengthening your organization’s cyber security requires a comprehensive approach that extends beyond email-specific strategies. In this section, we explore additional cyber security best practices that complement email protection efforts. By implementing these measures, you can improve your security posture and protect your digital assets from various threats.

3.3.1 Use unique and strong passwords or passphrases

Create unique and strong passwords and passphrases for your accounts. Do not repeat or reuse passwords and passphrases for multiple accounts and consider using a password manager to securely store your passwords and passphrases. You should aim to create complex and resilient passwords/passphrases, as attackers frequently exploit weak ones. For more information on best practices for passwords and passphrases, read Best practices for passphrases and passwords (ITSAP.30.032) and Rethink your password habits to protect your accounts from hackers (ITSAP.30.036).

For tips on using password managers, consult Password managers: Security tips (ITSAP.30.025).

3.3.2 Educate and train employees

Employee education and security awareness training are essential components of an effective enterprise email security strategy. It is important that employees at all levels understand the value of protecting sensitive data and the repercussions of emails attacks and breaches. Employees are the initial line of defence within organizations, which underscores the need for regular and comprehensive security training to mitigate the risk of human errors. The more knowledgeable your employees are about email security, the less likely they are to fall victim to threat actors' tactics and to scams.

Here are some keys aspects to consider incorporating into your training:

- techniques to identify and avoid phishing, ransomware, and BEC attacks
- strategies for avoiding security threats like malware, malicious links, and attachments
- ways to ensure the security of sensitive information
- data classification and handling procedures
- tips for protecting passwords
- guidelines on responding to email account compromises and promptly reporting suspicious emails or security incidents
- risks associated with phone-number compromise (subscriber identity module (SIM) swapping)
- reasons why the crossover use of work and personal emails should be prohibited
- suitable file types for email transmission and secure file-transfer methods
- techniques for detecting social engineering attempts and for knowing what not to share through email or other communication channels
- organization-specific email security policies and industry regulations

The goal is to empower employees by providing comprehensive information and to improve organizations' overall email security posture.

3.3.3 Use multi-factor authentication

Use MFA whenever possible to secure your email account. MFA helps prevent unauthorized access to accounts, even if your password has been compromised. While strong passwords are beneficial, MFA adds an extra layer of access control since it requires you to provide more than just a password to login. MFA requires a user to provide 2 or more different authentication factors to verify their identity during a login process. These authentication factors can be a combination of something the user knows (for example, password or PIN), something the user has (for example, a smart card or a security key), or something the user is (biometric features such as fingerprint or face scan). This makes it harder for threat actors to gain unauthorized access to your accounts, especially email containing sensitive information.

Phishing-resistant MFA refers to multi-factor authentication methods that are designed to be resilient against phishing attacks. These methods typically do not rely on shared secrets like passwords or codes that can be intercepted or stolen through phishing. Instead, they use cryptographic authentication that does not expose reusable credentials to service providers or attackers.

One example of phishing-resistant MFA technology is Fast Identity Online (FIDO) based solutions. FIDO uses cryptographic login credentials that are unique to each website and are never stored on a server.

To learn more about MFA, read our publications Secure your accounts and devices with multi-factor authentication (ITSAP.30.030) and Steps for effectively deploying multi-factor authentication (MFA) (ITSAP.00.105).

3.3.4 Keep software and operating systems updated

Regularly updating your email security software, anti-virus programs, and operating systems (OS) is important to bolster the security of your email system and protect against identified vulnerabilities. Threat actors often capitalize on weaknesses in outdated software to attain unauthorized access, steal data, or damage your computer. Since major operating systems usually have built-in anti-virus software, you should enable automatic updates for the operating system and any supplementary anti-virus tools to ensure you have the latest security patches. For more information on the importance of updates, read our publication How updates secure your device (ITSAP.10.096).

3.3.5 Connect to reliable Wi-Fi networks

Whenever possible, you should refrain from using public Wi-Fi for email communication. These networks are enticing targets for hackers, who may try to access or steal sensitive information when you are online. If you must connect to public Wi-Fi, exercise caution to prevent threat actors from intercepting your email data. Be selective about the Wi-Fi networks to which you connect. Prioritize public Wi-Fi connection options to those with secure encryption such as Wi-Fi protected access 3 (WPA3) or, even better, WPA3 with simultaneous authentication of equals-public key (SAE-PK) when possible. If you need to access sensitive email information, use a virtual private network (VPN) to establish a secure connection and protect data. However, you should be aware that not all VPN services offer the same level of trustworthiness. You should choose a VPN provided by a trusted organization rather than relying on publicly available VPN services. For more on Wi-Fi security, read our publications Wi-Fi security (ITSP.80.002) and Protecting your organization while using Wi-Fi (ITSAP.80.009).

3.3.6 Create an incident response plan

Organizations should develop and regularly update an incident response plan that includes responding to email security incidents. This plan should outline the specific actions to be taken in the event of an email security incident. This includes isolating affected systems to prevent further damage, identifying and mitigating vulnerabilities that may have been exploited, and notifying relevant stakeholders, such as IT teams, management, and possibly even affected users. For information on how to create an incident response plan, read our publication Developing your incident response plan (ITSAP.40.003).

3.3.7 Back up important files

Ensure the security and availability of your emails by routinely backing them up to protect against accidental deletion, hardware failures, or security breaches. Explore cloud-based backup solutions, local backup, or isolated solutions to identify what aligns best with your organization's needs. Consider backing up critical files in multiple locations and in backup systems isolated from the primary network. This will prevent ransomware or other malware from easily spreading to the backup infrastructure. Conduct regular restoration exercises to verify the integrity and effectiveness of your backup systems. This practice helps identify any potential issues in the backup process and ensures a smooth recovery in the event of a cyber attack. For guidance on backing up your files, read our publication Tips for backing up your information (ITSAP.40.002).

3.4 Engaging with email security experts

Organizations seeking advanced email protection or those that do not have the in-house expertise should consider engaging with a reputable email security expert or adopting a cloud-based solution. Third-party email security service providers can offer a multilayered defence solution with advanced threat intelligence, robust filtering, real-time monitoring, proactive threat detection, and rapid response capabilities. These services can include detailed reporting and analytics to support compliance efforts, identify vulnerabilities, and provide insights into email security trends. For some organizations, outsourcing can help optimize resource allocation, reduce the burden on internal teams, and ensure a comprehensive defence against cyber threats.

To ensure that third-party email security services adequately protect your email and sensitive information, apply a supply-chain-integrity analysis. This involves conducting thorough assessments and due diligence on the provider's security practices, infrastructure, and adherence to industry standards and regulations. Verify the provider's track record, certifications, and any relevant security audits or assessments. This process ensures that third-party services will sufficiently safeguard your data, reducing risks associated with outsourcing. For more on supply chain integrity, read our publications Cyber supply chain: An approach to assessing risk (ITSAP.10.070) and Protecting your organization from software supply chain threats (ITSM.10.071).

Below is a list of the various types of email security services to consider.

3.4.1 Detonation and email sandboxing

In the context of email security, detonation involves executing potentially harmful email attachments or links within a controlled environment to analyze their behavior and determine if they pose a threat. This process, also known as email sandboxing, occurs within a secure and isolated environment and allows security professionals to scrutinize suspicious files without risking harm to the organization's network or systems. By observing the attachment's actions in this controlled setting, security teams gather valuable intelligence to better understand and mitigate cyber security risks.

3.4.2 Content control

Content control in email security services involves the use of advanced technologies like AI and machine learning (ML) to analyze email content for unsafe patterns. These services can identify and block various types of potentially harmful content. Specifically, image and content control capabilities focus on scanning attached or embedded images and content within emails. By leveraging AI and ML, these services can detect malware in images and content and prevent their download or execution.

Spam and phishing filters are designed to automatically identify and block potentially malicious emails. Third-party services enhance spam and phishing detection by employing advanced algorithms and threat intelligence to analyze email content and sender behavior so that phishing attempts can be identified and blocked before they reach users' inboxes. These filters also block emails with attachments attempting to access system registries or sensitive folders, as well as those trying to communicate with external IP addresses or download files from external sources. Overall, these measures contribute to a strong defence against spam, phishing, and potential security threats in email communications.

In addition to AI, ML, and spam and phishing filters, you can leverage the following traditional methods for effective email content filtering and to block or quarantine suspicious attachments or file types:

- Use email server features to block or quarantine suspicious attachments or file types
- Implement allow lists to permit only safe file types, thereby enhancing security
- Automatically convert MS Office documents or other types of documents containing macros to safer formats like PDF to mitigate the risks associated with malicious macros
- Remove or disable active content to prevent exploitation
- Deploy anti-virus and anti-malware software to scan email attachments for threats, including archive files like Zip, Rar, and 7zip, which may be quarantined or removed if encrypted
- Disable macros in MS Office documents if they are allowed, as macros are a common attack vector

3.4.3 Authentication systems

Authentication systems are essential for defending against spoofed emails, ensuring the legitimacy of senders, and mitigating various cyber threats.

Anti-spoofing tools use email authentication protocols to prevent impersonation attacks and flag or reject suspicious messages. Third-party services support organizations in implementing and managing authentication protocols such as SPF, DKIM, and DMARC. The primary aim is to prevent domain spoofing, flag or reject suspicious messages, and guarantee the authenticity of email communication, thereby reducing the risk of cyber threats.

3.4.4 Email encryption

Email encryption is a security measure that uses encryption techniques to effectively mitigate the risk of email interception. Encrypted emails, which can only be read by authorized senders and recipients, play a pivotal role in preventing unauthorized access to and interception of sensitive information.

Email security service providers offer strong email encryption solutions to enhance the security of your sensitive information during transmission. These solutions encompass a range of encryption protocols and advanced push-and-pull encryption methods. With push encryption, emails are converted into encrypted files attached to another email, ensuring secure transit and restricting access to authorized recipients. Pull encryption enables secure email retrieval from a designated portal, ensuring access solely for individuals with the appropriate credentials. These measures collectively safeguard your emails from unauthorized access and ensure the confidentiality of your communications.

3.4.5 Email security gateways

Email security gateways are another service offered by email security experts. By deploying these gateways, email security experts ensure that all incoming and outgoing emails are thoroughly inspected, blocking malicious content, and safeguarding your communication channels.

3.4.6 Continuous monitoring

There are email security services that continuously monitor and gather threat intelligence to help defend against emerging threats and vulnerabilities. These services actively monitor the email landscape, watch for new attack vectors, and adapt quickly to evolving risks. By using threat intelligence, they are better able to deliver timely and effective protection against emerging cyber threats.

3.4.7 Reporting and analytics

Email security tools that provide reporting and analytics include features for monitoring email traffic and tracking security incidents. Through these capabilities, organizations acquire valuable insights into potential security threats, which allow them to proactively address vulnerabilities. The tools produce detailed reports that provide a comprehensive view of the email security landscape and help organizations identify patterns, trends, and areas that may need additional attention.

4 Summary

It is important for your organization to safeguard emails containing sensitive data, including financial records, proprietary information, and customer and employee details. One key way of doing this is to implement comprehensive email security best practices, including elements such as encryption, authentication, secure gateways, monitoring, and regular audits. Adopting these practices not only ensures a robust defence against potential breaches, but also protects the confidentiality of sensitive information during email transmission.

Email security protocols, including TLS, S/MIME, SPF, DKIM, and DMARC, play pivotal roles in strengthening email communication security. These protocols address diverse aspects of cyber security, such as encryption, authentication, and protection against phishing and spoofing attempts.

Adhering to these security protocols and the best practices covered in this document will help your organization establish a trustworthy communication environment, especially in transactions involving sensitive data. Collectively, they can help strengthen your organization's overall data privacy strategy, improve its security posture, and increase resilience. By prioritizing email security, organizations not only instill confidence in stakeholders but also foster a culture of cyber security awareness and maintain a proactive stance against emerging cyber threats.