EXPERT GUIDE

Email Security Best Practices for MSPs

14 Things Cyber Insurance Providers Look For

mailprotector

ABOUT THE GUIDE

Discover 14 essential **Email Security Best Practices for MSPs** to safeguard your clients' digital assets while playing nice with cyber insurance providers.

Thank you for downloading this eBook!

BEST PRACTICES FOR MSPs
EMAIL SECURITY

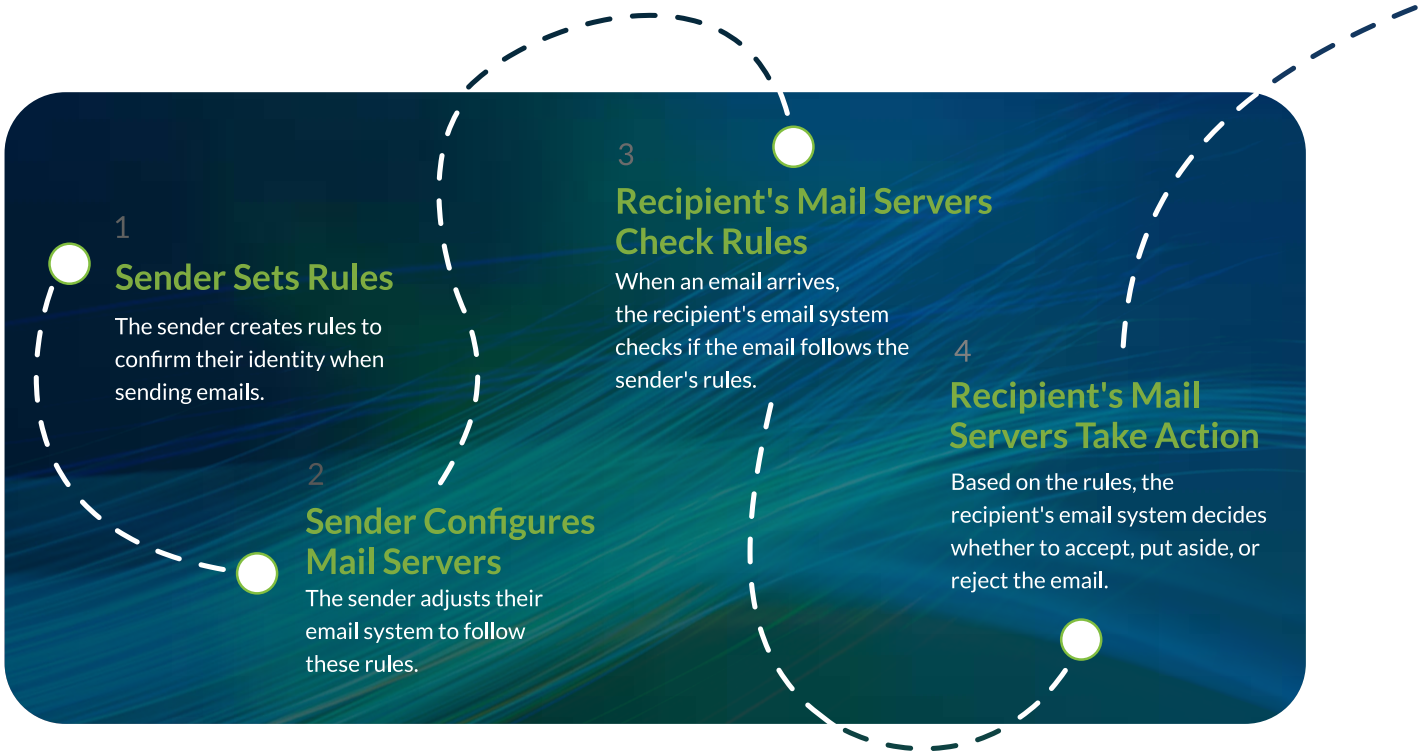
Throughout this book, you'll explore a comprehensive set of best practices ***that any MSP can employ*** to fortify their clients' email defenses. From encryption and authentication protocols to employee training and threat detection, this guide will equip you with the knowledge and tools to better serve as a trusted security advisor.

You can use the following list of 14 email security best practices to help your clients achieve cybersecurity maturity and improve their eligibility for cyber insurance.

14 Email Security Best Practices for MSPs

Helping your clients understand and follow these best practices will help your MSP demonstrate its commitment to mitigating their cyber risks — a factor that can influence insurers to offer more favorable terms and coverage options, and help you sell more types of email security products.

In the next few pages, we highlight some of the key fundamental components to an absolute email security approach starting with Email Authentication.



Email Authentication

FUNDAMENTAL COMPONENT OF EMAIL SECURITY **#01**

Authentication ensures that the sender of an email is who they claim to be. Common authentication methods include Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC).

Maintain your cyber insurance coverage eligibility by having authentication security rules in place. Only authorized users will be able to send and receive emails, preventing unauthorized access and reducing the risk of email-based attacks.

ACTION ITEMS

- [ ] Configure SPF Records
- [ ] Set Up DKIM Signatures
- [ ] Enable DMARC Policy Enforcement
- [ ] Monitor and Fine-Tune Authentication Policies
- [ ] Provide Ongoing Support and Training
- [ ] Conduct Regular Audits to Ensure Effectiveness

Email Encryption

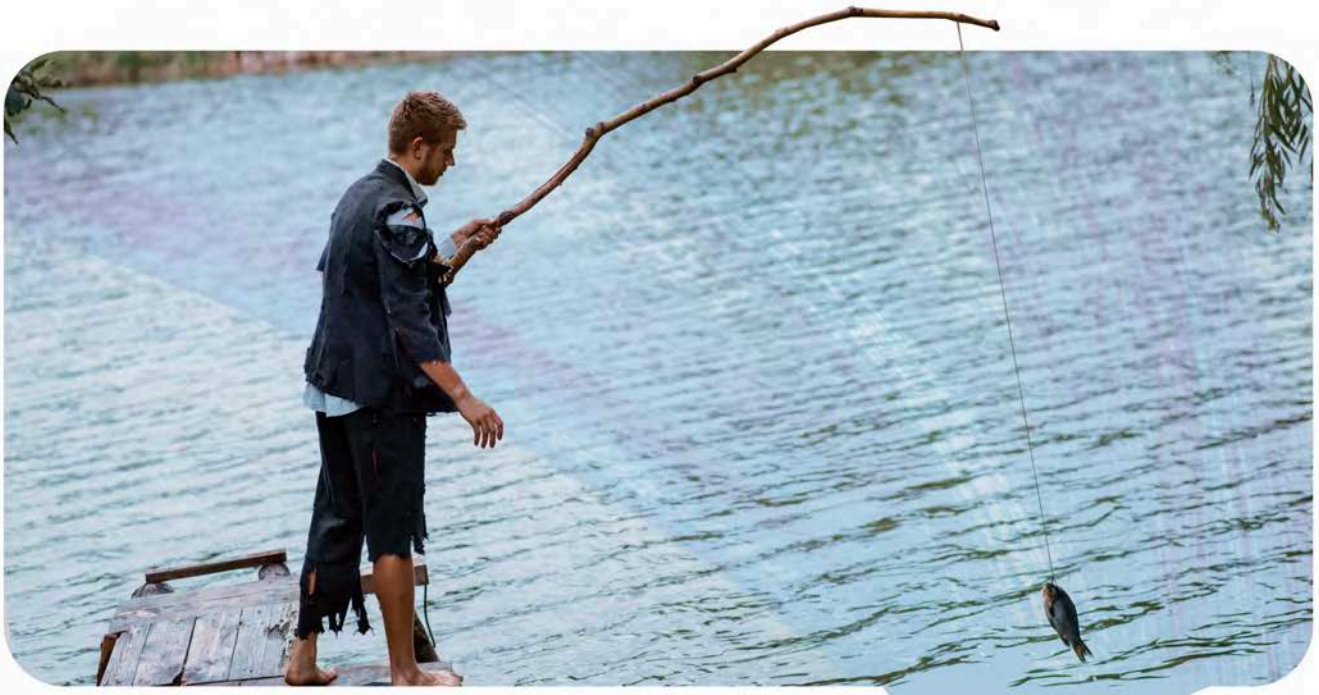
FUNDAMENTAL COMPONENT OF EMAIL SECURITY **#02**

Encrypting emails with methods like Transport Layer Security (TLS) and end-to-end encryption ensures only the intended recipient can access them. By encoding content, email encryption prevents unauthorized access, data breaches, compliance issues, and other cyber threats.

Robust encryption practices demonstrate proactive data protection, potentially reducing security risks and lowering insurance premiums. Insurers value organizations with strong encryption measures, as they signify a lower likelihood of costly security incidents, leading to potential cost savings and enhanced insurance coverage for these organizations.

ACTION ITEMS

- [ ] Deploy Transport Layer Security (TLS)
- [ ] Implement End-to-End Encryption
- [ ] Implement a Secure Email Gateway (SEG)
- [ ] Enable Email Encryption Policies
- [ ] Provide Client Training and Support
- [ ] Regularly Monitor & Audit Encryption Practices



Phishing Protection

FUNDAMENTAL COMPONENT OF EMAIL SECURITY **#03**

Phishing protection entails the deployment of intricate filters and detection mechanisms integrated into email security systems to discern and intercept malicious emails. Leveraging sophisticated algorithms, these solutions meticulously scrutinize email content, attachments, and sender attributes, swiftly identifying suspicious messages and halting their progression to users' inboxes.

Phishing protection is crucial for cyber insurance providers as it mitigates the risk of successful email-based attacks like business email compromise and ransomware, bolstering an organization's security posture and potentially reducing insurance premiums.

ACTION ITEMS

- [ ] Implement Advanced Email Filtering
- [ ] Deploy Email Authentication Protocols
- [ ] Enable Multi-Factor Authentication
- [ ] Conduct Regular Phishing Awareness Training
- [ ] Establish Clear Incident Response Procedures
- [ ] Utilize Secure Gateways

Spam Filtering

FUNDAMENTAL COMPONENT OF EMAIL SECURITY **#04**

Spam filtering is like a virtual gatekeeper for your email inbox, working behind the scenes to keep out unwanted and potentially harmful emails. By carefully inspecting email content, checking the reputation of senders, and considering other important factors, spam filters act as a shield to help mitigate the risks associated with phishing attacks and malware distribution, creating a safer email environment for organizations.

Comprehensive spam filtering not only reduces the risk of email-based cyber threats but also showcases an organization's dedication to cybersecurity. Insurers may penalize or deny coverage to entities without this protection, given the increased susceptibility to malicious email attacks.

ACTION ITEMS

- [ ] Implement Advanced Spam Filtering
- [ ] Configure Email Server Settings
- [ ] Regularly Update Spam Filter Rules & Definitions
- [ ] Utilize a Secure Email Gateway
- [ ] Implement Sender Authentication Protocols
- [ ] Monitor Spam Filter Logs and Reports

Anti-Malware Scanning

FUNDAMENTAL COMPONENT OF EMAIL SECURITY **#05**

Email security systems scan attachments and links within emails for malware, viruses, and other malicious content. If a threat is detected, the email or the malicious content is quarantined or blocked.

Having anti-malware scanning implemented demonstrates proactive measures to mitigate the risk of malware-related incidents, thereby reducing the likelihood of financial losses and reputational damage. Cyber insurance provides coverage for expenses related to malware attacks, such as forensic investigations, data recovery, legal fees, and ransom payments, offering financial protection and peace of mind in the event of a security breach.

ACTION ITEMS

- [ ] Implement Email Scanning
- [ ] Configure Real-Time Scanning
- [ ] Schedule Regular Scans
- [ ] Enable Automatic Updates
- [ ] Monitor and Respond to Alerts
- [ ] Establish Quarantine Procedures & Policies

Secure Email Gateway (SEG)

FUNDAMENTAL COMPONENT OF EMAIL SECURITY **#06**

A Secure Email Gateway is like a vigilant guardian stationed at the entrance to your email system, continuously monitoring incoming and outgoing emails for potential threats before they reach your inbox. Having a SEG is vital for maintaining a secure email environment by adding an extra layer of protection against cyber threats.

By having a SEG in place, businesses can prevent harmful emails from reaching their employees' inboxes, reducing the risk of cyber incidents. This lowers the chance of needing to make insurance claims for damages caused by email-based attacks, potentially leading to lower insurance premiums and ensuring better coverage overall.

ACTION ITEMS

- [ ] Implement a Secure Email Gateway (SEG)
- [ ] Deployment Planning (On-Prem, Cloud, Hybrid)
- [ ] Configuration and Integration
- [ ] Testing and Optimization
- [ ] Develop & Implement Email Security Policies
- [ ] Training and Documentation

Data Loss Prevention (DLP)

FUNDAMENTAL COMPONENT OF EMAIL SECURITY **#07**

Data Loss Prevention (DLP) for email security acts as a safeguard, securing sensitive information such as policy details, payment records, and personal identifiers like Social Security numbers do not leave an organization without permission.

Insurance providers are looking for DLP to stay in compliance with industry regulations such as HIPAA and GDPR, mitigating the risk of costly fines and preserving trust with policyholders by preventing unauthorized access or inadvertent leaks of this data.

ACTION ITEMS

- [ ] Enable Email Encryption
- [ ] Implement Email Filters
- [ ] Identify and Classify Sensitive Data
- [ ] Create DLP Policy
- [ ] Use Strong Authentication
- [ ] Monitoring & Updates

Email Backup & Recovery

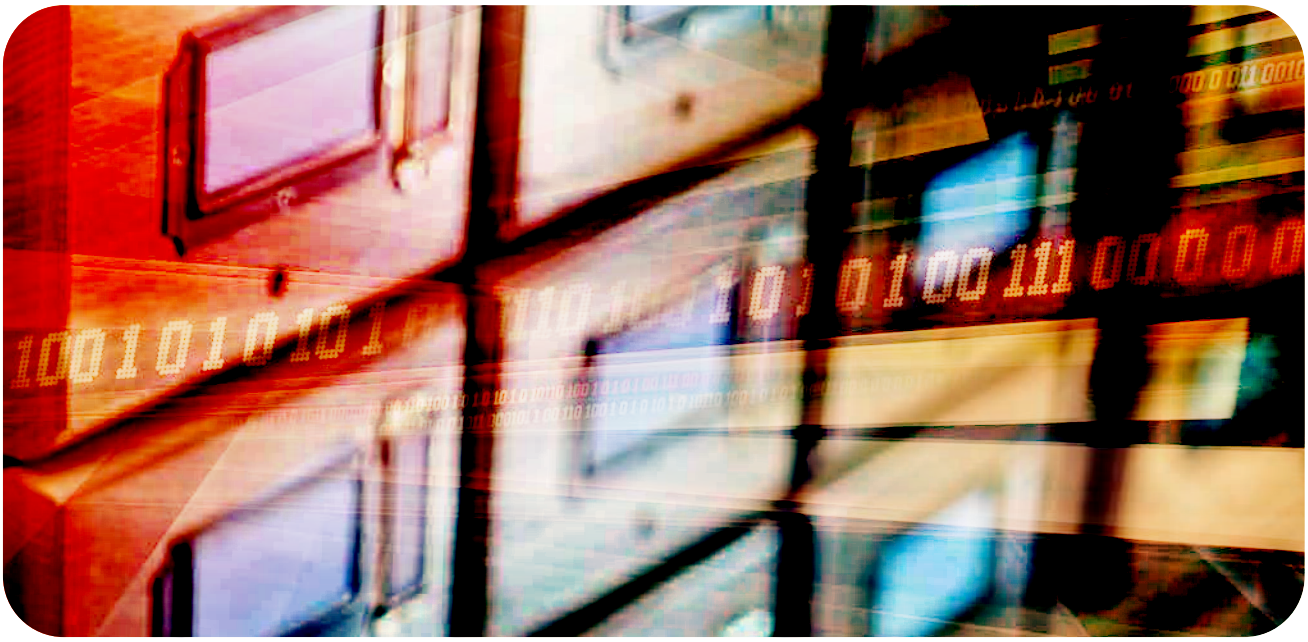
FUNDAMENTAL COMPONENT OF EMAIL SECURITY **#08**

This step is critical in the event of data loss, whether due to accidental deletion, cyberattacks, hardware failures, or other unforeseen incidents. By regularly backing up email data and having a recovery plan in place, organizations can secure the continuity of their email services and quickly restore lost or compromised emails.

Email backup and recovery are vital for cyber insurance providers because they preserve critical communication records and evidence required for investigating cyber incidents and processing claims. Insurers can reconstruct an event's timeline and assess the extent of the damage.

ACTION ITEMS

- [ ] Identify and Prioritize Critical Email Data
- [ ] Define Backup Policies
- [ ] Implement Backup Automation
- [ ] Test Backup and Recovery Processes
- [ ] Secure Backup Data
- [ ] Monitor and Document Backup Procedures



Email Archiving

FUNDAMENTAL COMPONENT OF EMAIL SECURITY **#09**

Archiving is often required by data security and privacy regulations for compliance and legal purposes. In cases where it's not mandated, this feature or service is useful for record retention and risk mitigation by storing and managing emails in a centralized repository for long-term retention and retrieval purposes.

Email archiving is essential for cyber insurance providers to accurately assess and process claims related to cyber incidents, as it provides crucial evidence of communication timelines and exchanges. Additionally, it ensures compliance with regulatory requirements regarding data retention and disclosure obligations, enhancing transparency and trustworthiness in insurance operations.

ACTION ITEMS

- [ ] Develop Clear Archiving Policies and Procedures
- [ ] Configure Archiving System To Defined Policies
- [ ] Implement Automated Archiving
- [ ] Provide Training and Education
- [ ] Monitor Archiving Systems
- [ ] Develop a Disaster Recovery Plan

Software Updates & Patching

FUNDAMENTAL COMPONENT OF EMAIL SECURITY **#10**

Maintaining a secure email environment requires regular software updates and patching. Software updates refer to the release of new and improved versions of the software that operates your email systems, such as email clients or servers. These updates often include critical security fixes and patches to strengthen your defenses against cyber threats. These patches act as digital band-aids, covering weaknesses in the software's code and making it more resilient to cyber threats.

Keeping your email clients and server software up-to-date is crucial for cybersecurity and passing insurance audits. By demonstrating a commitment to maintaining a secure email environment through regular updates and patching, businesses can improve their cybersecurity posture and potentially qualify for better insurance terms and coverage options.

ACTION ITEMS

- [ ] Develop Patch Management Policy
- [ ] Implement Automated Update Notifications
- [ ] Test Patches in a Controlled Environment
- [ ] Utilize Vulnerability Scanning Tools
- [ ] Prioritize Critical Security Patches
- [ ] Develop a Rollback Plan to Revert Changes

User Education & Training

FUNDAMENTAL COMPONENT OF EMAIL SECURITY **#11**

Users are key to protecting sensitive information and are often targeted by cybercriminals. Teaching users about email security best practices helps them recognize threats like phishing attempts and avoid suspicious links or attachments, reducing the risk of data breaches and cyberattacks. Informed users = safer email.

User education and training take on added importance as they directly impact an organization's risk profile and insurability. Insurance providers often consider the level of user awareness and adherence to security protocols when underwriting cyber insurance policies. Investing in comprehensive training programs demonstrates a commitment to mitigating cyber risks, potentially reducing insurance premiums, and ensuring adequate coverage in case of a security incident.

ACTION ITEMS

- [ ] Conduct Security Assessment
- [ ] Develop Policy Documentation
- [ ] Create a Customized Training Plan & Schedule
- [ ] Perform Incident Response Training
- [ ] Continuous Monitoring & Improvement
- [ ] Schedule Regular Training Sessions

Monitoring & Auditing

FUNDAMENTAL COMPONENT OF EMAIL SECURITY **#12**

Continuous monitoring and auditing of email traffic is essential for maintaining the integrity of communication channels, detecting security threats, and safeguarding sensitive information. This bolsters security measures and ensures compliance with regulatory standards and data protection laws.

Implementing robust email monitoring and auditing measures significantly enhances an organization's cybersecurity posture, thereby increasing the likelihood of attaining comprehensive cyber insurance coverage. By demonstrating proactive risk management and adherence to best practices, organizations can present themselves as lower-risk candidates to insurance providers, potentially leading to more favorable coverage terms and premiums.

ACTION ITEMS

- [ ] Assess Current Email Systems
- [ ] Research and Select Monitoring Tools
- [ ] Define Monitoring Parameters
- [ ] Establish Comprehensive Audit Protocols
- [ ] Implement Automation for Efficiency
- [ ] Provide Staff Training and Awareness

Incident Response Planning

FUNDAMENTAL COMPONENT OF EMAIL SECURITY **#13**

As an MSP, working with your clients to create detailed incident response plans is a best practice. This involves gathering input from relevant stakeholders, assessing the organization's specific needs and requirements, and collectively outlining the framework for incident response. This plan should include steps to contain, investigate, and mitigate any potential breaches while defining how they will work with you to resolve the situation.

Cyber insurance policies typically include provisions for incident response and recovery. An organization with a solid incident planning and response strategy may be better equipped to respond to and recover from email-based cyber incidents, leading to more effective use of insurance resources in case of a breach.

ACTION ITEMS

- [ ] Collaborate with Clients on Plan Development
- [ ] Define Incident Containment Procedures
- [ ] Establish Investigation Protocols
- [ ] Implement Breach Mitigation Steps
- [ ] Outline Protocols for Incident Response
- [ ] Test and Update Plan Regularly

Ongoing Security Policy Updates

FUNDAMENTAL COMPONENT OF EMAIL SECURITY **#14**

The cyberthreat landscape is constantly changing and your security posture must adapt in kind. Regularly reviewing and updating email security policies and procedures is crucial to adapting to evolving threats, ensuring the continued effectiveness of security measures, and protecting sensitive information.

By demonstrating proactive measures in regularly reviewing and updating email security policies and procedures, organizations not only strengthen their cybersecurity resilience but also enhance their attractiveness to cyber insurance providers, potentially leading to more comprehensive coverage options and reduced financial risks associated with cyber incidents.

ACTION ITEMS

- [ ] Schedule Regular Policy Reviews
- [ ] Stay Informed About Emerging Threats
- [ ] Engage Stakeholders from Various Departments
- [ ] Conduct Risk Assessments Regularly
- [ ] Update Policies Based on Assessment Findings
- [ ] Ongoing Training on Roles & Responsibilities

Stay Positive, Stay Secure.

MSPs and their approach to email security has never been more imperative. As cyber threats continue to evolve and become increasingly sophisticated, MSPs must remain vigilant in implementing best practices to protect their clients' email systems. Our ebook has highlighted essential strategies and technologies that MSPs can adopt to enhance email security effectively.

From understanding the importance of comprehensive email security solutions to deploying advanced threat detection mechanisms, MSPs play a pivotal role in fortifying their clients' defenses against cyberattacks. And it's MSPs that can help significantly reduce the risk of email-based threats by emphasizing and enforcing proactive measures such as employee training, regular security assessments, and robust incident response plans.

Furthermore, the symbiotic relationship between email security and cyber insurance providers cannot be overstated. As the email security health posture of organizations directly impacts their risk profile, cyber insurance providers rely on MSPs to uphold high standards of security. A strong email security posture not only mitigates the financial and reputational risks associated with cyber incidents but also ensures compliance with regulatory requirements.

In today's digital age, where email remains a primary communication channel for businesses, MSPs must continuously adapt and innovate their email security strategies. What was once “good enough,’ is no longer. Email is still the most targeted by threat actors. By staying informed about emerging threats, leveraging cutting-edge technologies, and fostering a culture of cybersecurity awareness, you can position yourself as a trusted partner in guarding clients' sensitive data.

We hope this ebook has provided valuable insights and actionable recommendations to enhance your email security practices for your own MSP and your clients. By implementing these best practices, MSPs can build resilience against cyber threats, protect their clients' assets, and contribute to a safer digital ecosystem for all.

Remember, email security is not just a checkbox; it's a dynamic and ongoing process that requires collaboration, expertise, and dedication. We appreciate your commitment to exploring the intricacies of email security and the role MSPs have in securing the email landscape, and we look forward to seeing the continued advancements in email security across the industry.

Jump to the next page to get started with a free tool that allows you to check the vulnerability of your and your clients' emails.

Radar™

Check your six

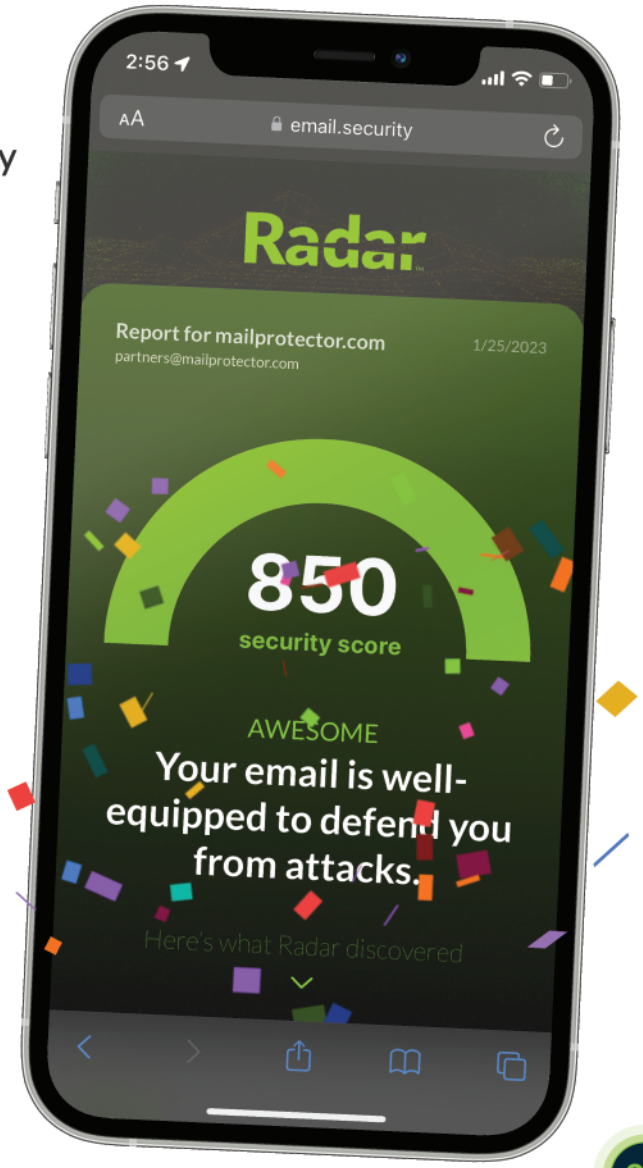
Are you vulnerable to an email attack? Get your email security score and know if you're an easy target.

What's your email? | Start test →

Your email will only be used for your security test. This site is protected by reCAPTCHA. Privacy and Terms apply.

Start with **Radar**, a free comprehensive email security test that takes a deep look into your email and brings to light the hidden security flaws you might not even know are there.

There's no need to download or install anything; you can test on any device. Just follow the three steps below:



VISIT

https://email.security

START

Submit your email to fire off a test of your incoming email systems

REPLY

Hit “reply” and “send”, that’s it.

REPORT

Wait a few moments, then recheck your inbox for the link to your report.

ARE YOU SECURE?

Radar™

Because **Radar** employs an entire email delivery loop to check 9 critical areas for issues, we can provide a complete 360-degree security analysis of both your incoming and outgoing email. Our report gives you meaningful, data-driven action items you can use to fortify your domain against email threats.

What's the catch? There isn't one; we simply want everyone to experience email safely, the way it was intended.

Factors	Max: 850
Receive email with (TLS) encryption	150
Send email with (TLS) encryption	150
MX records do not expose email host	100
DomainKeys Identified Mail (DKIM)	100
Sender Policy Framework (SPF)	100
Domain/IP reputation	100
Domain-based Message Authentication Reporting and Conformance (DMARC)	75
Reverse DNS	50
Email spy tracking	25
	Total: 850

CHECK YOUR EMAIL SCORE

Better yet, run it on your client domains and to show them gaps in their email security posture.

Improve your score

We strongly recommend that you make the following changes to get a better score and greatly improve the safety of the people who use email at your domain. Once you make these changes, run Radar again to update your Security Score.

WARNING
Block email spy tracking
Leaking data by opening an email is a privacy and security risk. Use an email filtering service that identifies and removes pixel trackers from messages before they arrive in your mailbox. Then your privacy and security will be protected from email spies.

CRITICAL
Point hath.me MX records to a secure email gateway
Secure email gateways provide the highest level of protection for your email environment. By pointing your MX records at a secure email gateway, you stop email threats at the perimeter and hide where your email is hosted.

CRITICAL
Setup an SPF record for hath.me
Sender Policy Framework (SPF) is used to authenticate the sender of an email. With an SPF record in place, Internet Service Providers can verify that a mail server is authorized to send email for a specific domain. An SPF record is a DNS TXT record containing a list of the IP addresses that are allowed to send email on behalf of your domain.

CRITICAL
Setup DKIM for hath.me
DKIM stands for DomainKeys Identified Mail and is used for the authentication of an email that's being sent. A DKIM record exists in the DNS, but it is a bit more complicated than SPF. DKIM's advantage is that it can survive forwarding, which makes it superior to SPF and a foundation for securing your email.

CRITICAL
Setup DMARC for hath.me
Domain-based Message Authentication Reporting and Conformance (DMARC) is a free and open technical specification that is used to authenticate an email by aligning SPF and DKIM mechanisms. By having DMARC in place, domain owners large and small can fight business email compromise, phishing and spoofing.

CRITICAL
Use over-the-wire (TLS) encryption when receiving email
A properly configured email system supports opportunistic encryption. This means if encryption is available between two servers, it will use it to protect the data being transmitted. You should use an email service that supports this encryption.

CRITICAL
Use over-the-wire (TLS) encryption when sending email
A properly configured email system supports opportunistic encryption. This means if encryption is available between two servers, it will use it to protect the data being transmitted. You should use an email service that supports this encryption.

WARNING
Improve your domain or IP reputation
The domain or IP you're emailing from has a bad reputation. This means your emails are likely being blocked or put in the junk folder when they are delivered to people you email. We recommend you use an outbound email filtering service that provides you with protection for your reputation.

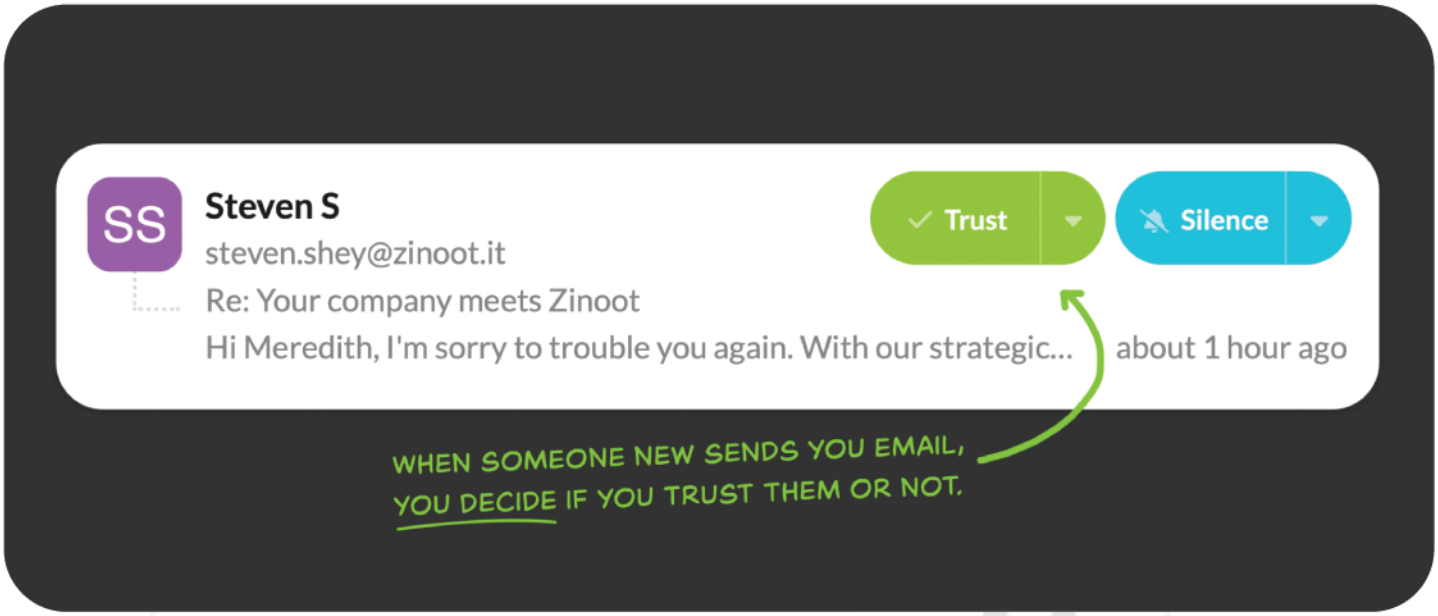
WARNING
Configure reverse DNS records
Most email services require proper reverse DNS records to be configured when relaying email. If your email service doesn't have this, it will negatively affect deliverability of email from your domain.

So... what's next?

Rather than assuming all emails are good and training machines to find bad ones, **next-gen email security** utilizes a zero-trust approach to stop all threats and noise by default.

Make an email earn its way into your inbox.

The result is a transformed email experience that changes how users safely and efficiently navigate their inboxes.



In a world where we spend too much time on email, Shield by Mailprotector steps in as more than just another filter. It's **three products in one...** combining intelligent inbound and outbound email protection with privacy and productivity features. Silence the noise and elevate your email to the powerful communication tool it was meant to be with Shield.

Protection
Brings superior protection directly to your inbox and works with any email client.

Privacy
The less a bad actor knows about you, the harder you are to attack.

Productivity
Gives you valuable time back by stopping all unwanted emails (not just the bad stuff).

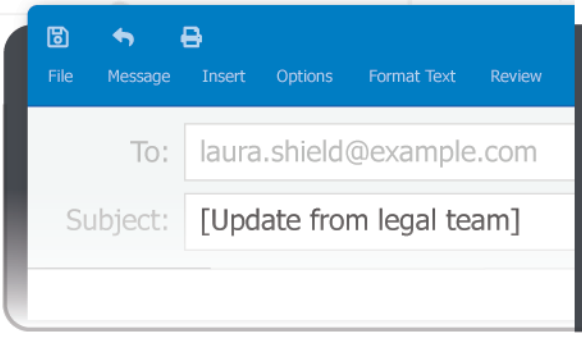
Shield your organization with absolute email security powered by AI.

Mailprotector's approach stands out by prioritizing your privacy and productivity alongside protection. Shield makes it harder for attackers to target you, and allows you to respond faster to what matters most.

We're eager to show you how Shield's intelligent, zero-trust technology can provide unmatched inbox security and peace of mind.

Schedule a demo today.

Mailprotector designs, builds, and support products that help organizations secure and optimize email. With former MSPs on staff, a beloved US-based partner success team, and a 100% channel focus you can rest easy knowing you are in the best of hands. Contact us today to see why MSPs worldwide ♥ Mailprotector.



[e] Bracket®

And don't forget about the easiest-to-use encryption tool on the market – Bracket. To encrypt a message, just wrap brackets around the [subject] and Bracket handles the rest.

THANK YOU!

We can't thank you enough for investing your time in reading our ebook on **MSP best practices for email security**, and your commitment to enhancing cybersecurity. We hope the insights provided in the ebook will help you strengthen your defenses.

LET'S RECAP

EXPERT GUIDE

Email Security Best Practices for MSPs

14 Things Cyber Insurance Providers Look For

mailprotector