Email Security Best Practices

Contents

Email Security Best Practice

This guide outlines Censornet's best practices for Email Security, these are based on our experiences with many customers and are in line with other industry best practices.

The following configuration recommendations will help you identify how to minimise your exposure to a range of email compromises to keep your organisation & users safe.

Our best practice advice covers a number of areas as summarised below.

Secure your Email Domains

- DMARC
- DKIM
- SPF
- Email Delivery Security

Protect your Users

- Active Directory Sync
- Executive Tracking
- Nearby Domain
- Display Name Detection
- External Email Warning Banner
- Advanced Sandbox
- Post Delivery Email Deletion (Retract)

Manage Admin Access

- MFA on Admin Account
- Admin Activity Audit

User Experience

- Outlook Plugin for M365
    - Report Spam/Phishing
    - Manage Quarantine
    - Manage Safe Sender Lists

Email Authentication - SPF

Feature: The Sender Policy Framework (SPF) is a DNS record added to the domain which specifies which hosts and IP addresses are allowed to send an email on behalf of a domain. The SPF system allows recipient email systems to check if the email was sent from a verified source, and if not, to act accordingly using the policy described in the SPF record.

Why do we recommend: To prevent spammers or hackers from sending messages on behalf of your domain

How to configure: Follow this KB article on how to configure this feature.

KB link - https://help.clouduss.com/ems-knowledge-base/mx-records-and-ip-addresses-for-all-regions

Tips:

- Ensure you are aware of the implications of the different options available with SPF records.

External References:

- https://en.wikipedia.org/wiki/Sender_Policy_Framework

Email Authentication - DKIM

Feature: DomainKeys Identified Mail (DKIM) is a DNS record added to the domain that stores the public key that the receiving email server uses to verify a message's signature. A DKIM includes a name, version, key type, and the public key itself, and is often made available by the provider that is sending your email.

Why do we recommend: Configuring DKIM on domains you send emails from is a stronger authentication mechanism than just SPF. It will help recipients validate the legitimacy of email which has passed through an email relay en route.

How to configure: Follow this KB article on how to configure this feature.

KB link - https://help.clouduss.com/ems-knowledge-base/configure-outbound-dkim

Tips:

- Ensure you are aware of the implications of the different options available with DKIM records.

External References:

- https://en.wikipedia.org/wiki/DomainKeys_Identified_Mail

Email Authentication - DMARC

Feature: Domain-based Message Authentication, Reporting and Conformance (DMARC) is a DNS record that is used to authenticate an email by aligning SPF and DKIM mechanisms.

Why do we recommend: Having DMARC in place can help to prevent business email compromise, phishing and spoofing attacks against your email domain.

How to configure: Follow this KB article on how to configure this feature.

KB link - https://help.clouduss.com/ems-knowledge-base/configure-outbound-dmarc

How it works: Follow this KB article on how DMARC works,

KB link - https://help.clouduss.com/ems-knowledge-base/how-does-dmarc-work

Tips:

- Please ensure you have both SPF and DKIM setup correctly before deploying DMARC.
- Ensure you are aware of the implications of the different options available with DMARC records.
- Although the DMARC KB uses p=none this is to start your DMARC journey, you should end up with a p=quarantine or p=reject policy for DMARC. By using p=none your domain may still be spoofed. This gives you the advantage of checking that real emails are not rejected or quarantined prior to making the change. You will get ruf reports of all failing emails which can help decide when you can go to this policy.

External References:

- https://en.wikipedia.org/wiki/DMARC
- https://www.ncsc.gov.uk/collection/email-security-and-anti-spoofing

LinkScan

Feature: LinkScan performs further checks on a URL within a delivered email at the moment the end-user clicks the link. In-depth redirect scanning and document detection are performed to confirm that the URL is safe for users to access.

Why do we recommend: By having Linkscan configured you will have a greater degree of security, this is because often it can take a while for threat intelligence feeds to report that an email is spam or has a malicious URL inside it.

How to configure: Follow this KB article on how to configure this feature.

KB link - https://help.clouduss.com/ems-knowledge-base/link-scan-on-demand-url-protection

Tips:

- You can set up rules based on AD groups to have a different LinkScan policy.
- The KB also include information on how to safelists senders or URLs if needed.

Active Directory

Feature: Active Directory Integration

Why do we recommend: By enabling Active Directory integration, you can create user-based filtering rules, either by AD User, AD Security Group or AD OU which can make creating filter rule logic a straightforward task.

How to configure: Follow this KB article on how to configure this feature.

KB link – https://help.clouduss.com/settings/active-directory

Tips:

- Get the most out of Active Directory integration by understanding our filter rules. KB link - https://help.clouduss.com/product-web-security/standard-rules#selected_conditions
- Use the API key method when synchronising from the on-prem Active Directory.

Executive Tracking

Feature: The Executive Tracking feature detects Business Email Compromise (BEC) attacks. A BEC attack sometimes called a "whale phishing" attack or CEO Fraud is a specific type of phishing attack that targets high-profile employees such as the CEO or CFO.

Why do we recommend: The attack intends to steal sensitive information from a company (since employees that hold high positions within the company will tend to request other users to complete certain tasks on their behalf). In many such attacks, the attacker's goal is to manipulate the victim into authorizing high-value wire transfers to the attacker.

How to configure: Follow this KB article on how to configure this feature.

KB link - https://help.clouduss.com/example-rules/executive-tracking

Tips:

- Use the send notification action to alert the intended target or the support team if the rule trigger.

Nearby Domain

Feature: The Nearby Domain feature detects if an attacker is sending an email with a similar domain in the email header to your domain. For example, a spam email delivered to **clouduss.com** may contain headers from **clouduus.com**.

Why do we recommend: The attack intends to steal sensitive information from a company (since employees that hold high positions within the company will tend to request other users to complete certain tasks on their behalf). In many such attacks, the attacker's goal is to manipulate the victim into authorizing high-value wire transfers to the attacker.

How to configure: Follow this KB article on how to configure this feature.

KB link - https://help.clouduss.com/example-rules/nearby-domain-rule

Tips:

- Use the send notification action to alert the intended target or the support team if the rule trigger.
- If you have a short domain i.e. abc.com then ensure the NBD value is set appropriately.

Display Name Detection

Feature: The Display Name Detection feature detects if an attacker is sending an email with unusual patterns in the display name; the area that shows who sent the email in most email clients. For example, some spammers will try and confuse filtering systems by using your real domain name inside the display name to try and convince the recipient the message is internal or genuine.

Why do we recommend: The attack intends to steal sensitive information from a company (since employees that hold high positions within the company will tend to request other users to complete certain tasks on their behalf). In many such attacks, the attacker's goal is to manipulate the victim into authorizing high-value wire transfers to the attacker.

How to configure: Follow this KB article on how to configure this feature.

KB link - https://help.clouduss.com/ems-knowledge-base/display-name-detection

Tips:

- Use the send notification action to alert the intended target or the support team if the rule trigger.

Post Delivery Email Deletion (Retract)

Feature: Post Delivery Email Deletion is a feature of Email Security that allows an administrator to delete email that has been delivered and stored in a Microsoft 365 / Office 365 mailbox, including any replies or forwards of the message within the domain.

Why do we recommend: This feature is particularly useful to delete and remotely wipe any messages accidentally released from quarantine or containing suspicious or confidential data.

How to configure: Follow this KB article on how to configure this feature.

KB link - https://help.clouduss.com/email-security/post-delivery-email-deletion-retract

Tips:

- View the admin audit log for this activity.

Advance File-based Sandbox (License Required)

Feature: Advanced Malware Scanning of file content.

Why do we recommend: The optional Advanced Email Sandbox protects against today's evasive zero-day threats by providing a highly scalable and powerful environment to run in-depth, sophisticated analyses of unknown or suspicious programs and files.

How to configure: Follow this KB article on how to configure this feature (only available if the Sandbox license has been purchased and applied).

KB link Overview - https://help.clouduss.com/email-security/email-sandbox-overview

KB link Configure - https://help.clouduss.com/email-security/product-configuration#sandbox_settings_add_on_product

Tips:

- You can disable or enable user notifications.

Email Delivery Security

Feature: Restrict email server to only receive inbound messages from Censornet

Why do we recommend: Attackers don't necessarily have to use MX records to deliver email. If email servers allow anyone to connect to them directly then Censornet EMS security checks can easily be bypassed.

How to configure: Follow these KB articles on how to best configure your environment.

KB link M365 - https://help.clouduss.com/email-security/email-sandbox-overview

KB link Googleworkspace - https://help.clouduss.com/ems-knowledge-base/configure-gmail-for-ems

KB link All Censornet IP Addresses - https://help.clouduss.com/ems-knowledge-base/mx-records-and-ip-addresses-for-all-regions

If you use an on-premise or hosted email server/service please ensure the Firewall is configured to only allow email delivery from Censornet's email servers.

Tips:

- Be aware of any legitimate services that send an email directly to your email service thus bypassing Censornet EMS. Determine whether all emails should be directed through Censornet or additional exceptions should be allowed for these services.

Safelisting EMS Security IP Addresses

Feature: Safelisting Censornet's IP ranges on your email service.

Why do we recommend: To ensure smooth delivery of email from EMS to your email service add a bypass rule that safelists Censornet IP addresses to stop your email service from causing unexpected results and behaviour for end users.

How to configure: Follow these KB articles on how to best configure your environment.

KB link M365 - https://help.clouduss.com/ems-knowledge-base/safelisting-email-security-ip-addresses-in-office-365

KB link Googleworkspace - https://help.clouduss.com/ems-knowledge-base/configure-gmail-for-ems

KB link All Censornet IP Addresses - https://help.clouduss.com/ems-knowledge-base/mx-records-and-ip-addresses-for-all-regions

Single Sign On with M365

Feature: Sign on to the USS portal with an M365 account.

Why do we recommend: This feature allows you to utilise a single identity source when accessing the USS portal.

How to configure: Follow this KB article on how to configure this feature.

KB link - https://help.clouduss.com/settings/single-sign-on

Tips:

- If any MFA settings are enabled on your M365 user account then these will be honoured.
- SSO will enhance the End User Portal role experience which is required for the SecureMail module and optional for end-user spam management.
- KB Link for End User Portal onboarding - https://help.clouduss.com/ems-knowledge-base/how-to-onboard-users-into-the-end-user-portal

External Email Warning Banner

Feature: Warning banner on external inbound email.

Why do we recommend: This feature allows you to notify users that the received email is from an external source and to apply caution.

How to configure: Follow this KB article on how to configure this feature.

KB link - https://help.clouduss.com/example-rules/how-to-prefix-a-banner-to-inbound-emails

Tips:

- Ensure the rule is in the correct location positioned at or near the top of your rule base.

Outlook plugin for M365

Feature: Outlook plugin for M365.

Why do we recommend: This feature allows users to report Spam and Phishing emails from their Outlook client.

How to configure: Follow this KB article on how to configure this feature.

KB link - https://help.clouduss.com/ems-knowledge-base/installing-the-outlook-add-in-for-reporting-spam-and-phishing-email

KB link upgrade for pre-December 2022 - https://help.clouduss.com/ems-knowledge-base/upgrade-outlook-add-in-for-reporting-spam-and-phishing-email

Tips:

- If you're unable to deploy the plugin due to the requirements then please send Spam or Phishing emails to spam@censornet.com as an attachment in EML format.

MFA on Admin account.

Feature: Enabling MFA on any admin account.

Why do we recommend: By enabling MFA on admin accounts, the authentication process will be improved by adding an extra layer of security via a simple SMS based OTP (One Time Passcode).

How to configure: Follow this KB article on how to configure this feature.

KB link – https://help.clouduss.com/settings/account-password-and-mfa

Tips:

- You can suspend users' accounts if they have not enabled MFA on their accounts.
- KB link Learn about types of admin roles - https://help.clouduss.com/settings/roles

Admin Audit License

Feature: Admin Audit license

Why do we recommend: By enabling the admin audit feature, administrators have a high-level history of activity carried out by administrator users within the **USS** dashboard?

How to configure: To check if you have the license, please view the kb article.

KB link – https://help.clouduss.com/account-settings/licenses