# Security Best Practices

Return Path, Inc.

## Table of Contents

## What is a secure database?

A secure database prevents others from tampering with your recipients' email addresses and related personal information.

## How do I secure sensitive data stored and passed over the internet and network?

To secure sensitive data stored or passed over an internet or network connection, follow these industry best practices:

- Enable reputable firewall hardware or software to protect your network.
- Allow remote access only through secure networks, such as Virtual Private Networks.
- Encrypt your wi-fi network, and hide its SSID; require a password for access.
- Encrypt files as they are transmitted over networks.
- Continually install and update security patches for your company's internal network.
- Install and configure antivirus/malware protection software; update regularly.
- Log and monitor significant computer and network security events, including password guessing attempts, hacking and virus incidents, and changes to system software.
- Require strong passwords to access company information systems, including laptops, smartphones, networks, and accounts.

## What are best practices for strong passwords?

To create strong passwords, follow these guidelines:

- Require at least eight characters
- Require the use of special characters (!, &, ?)
- Limit similarity to previous, current, and future passwords
- Limit password attempts
- Force password changes every 60-90 days
- Require numbers and the use of upper-case and lower-case letters

## How do I keep physical data secure?

To keep secure sensitive physical data, follow these industry best practices:

- Train your employees about your data security practices. Document and post your policies, and review them with all stakeholders.
- Limit access to sensitive information on a need-to-know basis.
- Ask employees to only open attachments or download software from trusted sources.
- When disposing of data, shred papers, and wipe out hard drives.
- Install encryption on all devices that contain sensitive information.
- Lock laptops when not attended, store files and removable storage devices containing sensitive information in a locked placed.

## What is a secure system?

A secure system prevents malware from breaking into your infrastructure. It also prevents open proxies or relays to allow unauthorized content to be sent from your IPs.

## How do I keep access to my servers secure?

Make sure access to your servers is on a need-to-have basis. To do this:

- Share access to your outbound email server with as few people as possible.
- Require strong passwords to access company information systems, including laptops, smartphones, networks, and accounts.
- Use two-factor authentication where possible.

## How do I configure my server to keep my systems secure?

To help keep your systems secure, configure them to do the following actions:

- Check DNS-based blacklists (DNSBLs), and reject email from any domains or IPs listed.
- Check Spam URI Real-time Block Lists (SURBL), and reject email from any messages containing invalid or malicious links.
- Maintain a local blacklist: a blacklist of IPs that target you, specifically.
- Keep total, simultaneous, and maximum connections to your SMTP server limited to prevent denial-of-service (DoS) attacks.
- Configure your system to default to a second MX (mail exchanger record) for each domain, in case one fails.

## What else do I need to do to keep my systems secure?

Along with the other best practices, do the following actions to keep your systems secure:

- Remove unneeded server functionality by disabling any unnecessary default settings.
- Continually install and update security patches for your company's internal network.
- EncryptPOP3 and IMAP authentication; use SSL and TLS.