1291 E. Hillsdale Blvd, Suite 303, Foster City, CA 94404
www.ittotalcare.com | Main: 650-352-6400

How to Improve Email Security: A Practical Guide for Home-Based Care Companies

Email plays a central role in how home-based care teams communicate, coordinate care, and manage sensitive information. That same reliance makes it one of the most targeted entry points for cyberattacks. A single compromised inbox can expose Protected Health Information, disrupt operations, and create serious compliance risks.

This guide outlines why email security is critical for home-based care companies, how to strengthen it internally, and how IT Total Care supports a more secure and compliant environment.

1. Why Email Security Matters for Home-Based Care Companies

Email security protects one of the most frequently used and most vulnerable systems in your organization. For home-based care teams, where communication happens across multiple devices and locations, email becomes a primary target for cyber threats.

Why It Matters for Home-Based Care Companies:

- **Phishing as the Leading Threat:** More than 90% of cyberattacks in healthcare originate from phishing emails, making inboxes the most common point of entry.
- **Protection of Sensitive Patient Data:** Email often contains PHI, care coordination details, and internal communications that must remain secure.
- **HIPAA Compliance Requirements:** Unsecured email systems can lead to violations, audits, and financial penalties if safeguards are not properly implemented.
- **Increased Risk in Remote Environments:** Care teams accessing email from mobile devices and home networks create more opportunities for attackers to exploit gaps.
- **Operational Continuity:** Preventing email-based breaches reduces downtime, avoids disruptions, and helps maintain consistent patient care.
- **User-Level Vulnerability:** Email attacks often succeed by targeting employees directly, making individual inboxes one of the easiest ways for cybercriminals to gain access to your systems.

For more information please contact,
Brendan Duebner | President | IT Total Care
Phone: (650) 425-3910 | Email: BrendanD@ITtotalCare.com

2. How to Improve Email Security Yourself

If you are managing email security internally, it is important to take a structured approach that covers both configuration and ongoing management. Here's a step-by-step approach that SMBs can follow:

Step 1: Select a Reliable Email Security Platform

- Research and implement a solution that includes spam filtering, threat detection, and protection against malicious links and attachments.

Step 2: Configure Email Authentication Protocols

- Enable SPF, DKIM, and DMARC records for your domain to prevent spoofing and improve email legitimacy.

Step 3: Establish Allow and Block Lists

- Whitelist trusted clients, partners, and vendors to avoid disruption while blocking known malicious senders.

Step 4: Monitor Email Activity and Alerts

- Regularly review flagged emails and system alerts to identify potential threats and respond quickly.

Step 5: Train Employees to Recognize Threats

- Educate staff on identifying phishing emails, suspicious links, and unusual requests to reduce human error.

Limitations: Managing email security internally can be inconsistent. Misconfigured authentication, missed alerts, or lack of user training can leave gaps that attackers will take advantage of.

For more information please contact,
Brendan Duebner | President | IT Total Care
Phone: (650) 425-3910 | Email: BrendanD@ITtotalCare.com

3. How IT Total Care Strengthens Email Security

As a Bay Area MSP, IT Total Care ensures your email security is not only implemented, but continuously managed and optimized.

Our Email Security Process Includes:

- **Advanced Email Filtering:** We deploy and manage spam filters that screen all incoming messages before they reach employee inboxes.
- **Authentication Configuration:** Our team sets up and maintains SPF, DKIM, and DMARC records to protect your domain from spoofing.
- **Ongoing System Tuning:** We work with your team to adjust filtering sensitivity and reduce false positives while maintaining strong protection.
- **Centralized Allow and Block Lists:** We manage approved and restricted senders across your organization to ensure consistency and control.
- **Suspicious Email Flagging:** We add disclaimers and alerts to help employees quickly identify potentially unsafe messages.
- **Spoofing Detection Alerts:** We configure real-time alerts for emails attempting to impersonate internal users or company domains.

Email security is one of the most important and often overlooked components of a strong cybersecurity strategy. For home-based care companies, it directly impacts patient privacy, regulatory compliance, and daily operations.

Ready to Strengthen Your Email Security?
At **IT Total Care**, we help home-based care companies implement and manage secure email environments that protect sensitive data and reduce risk. Our team handles configuration, monitoring, and ongoing optimization so your organization can operate with confidence.

For more information please contact,
Brendan Duebner | President | IT Total Care
Phone: (650) 425-3910 | Email: brendand@ittotalcare.com