Case Studies by Industry:

How does ITS' Email Security Bundle Protect our Clients?

ITS Integrated Telemanagement Services, Inc.
SIMPLIFYING TECHNOLOGY SINCE 1990

Health Care Provider

Issue: Client has Bracket for email encryption but sometimes the people sending emails forget to put the [Brackets] on confidential emails.

Solution: ITS configures rules that define the type of information that is considered "Confidential" and force encryption to be added automatically.

Result: This solution can save the provider from being fined for HIPAA violation of disclosing confidential information in a non-encrypted email.

ITS provides clients the peace of mind in knowing that their unique and custom email security policies are implemented and being actively enforced 24/7/365.

Church

Issue: In order to protect their reputation, this client has a policy against the use of profanity and wants to ensure that employees are not using it when sending emails from the church's domain.

Solution: Email security is configured to look for outgoing emails that contain defined profanity. If one is discovered, not only will it be only stoped before it goes out, but the Chaplin will be notified that the email was stopped.

Result: Chaplin is confident that the Church's reputation is in good hands with ITS and if an issue arises, it will be stopped and addressed before damage can be done. This also gives the Chaplin the opportunity to council the employee about policies.

Financial Institution

Issue: Cient has a policy that in order to protect their customers' data, Excel files cannot be emailed outside their business email domain.

Solution: By implementing email security rules, ITS was able to not only flag any emails that contained Excel documents as attachments but it also sent a notification to the CFO so that the employee could be reminded of the policy for sending out files.

Result: Client has peace of mind that only the appropriate types of files will be attached and sent outside their offices.

Email Security Bundle

- CloudFilter™ Total Email Security
- SafeSend™ Enhanced Outbound
- Bracket™ Encrypted Email

Case Studies by Industry:

Retail Store

Issue: Client just started accepting orders from their customers via email. In order to maintain PCI compliance they need to ensure that any emails they send to their customers confirming orders with credit card information are encrypted. Employees sometimes forget to follow this policy.

Solution: ITS configures rules that specify if credit card information is contained in an email to force encryption to be added automatically.

Result: This solution can save the provider from being fined for PCI violation of not properly handling credit card information.

Tax Preparer

Issue: In late 2019, the IRS started enforcing Tax Preparers data security requirement. By ensuring that any email communication that contains social security numbers are encrypted, the Tax Preparer will be one step closer to meeting those requirements.

Solution: ITS implements Bracket email encryption and then configures rules in SafeSend to automatically encrypt with Bracket any email that contains a social security or tax ID number.

Result: This solution can save the Tax Preparer from having their reputation tarnished due to data loss and being fined for Data Security violations due to not properly securing their clients data.

Cybersecurity Threats Across All Industries

Issue: An email comes into the Finance Assistant from the President of the company requesting urgent assistance with instructions for money to be transferred immediately to a defined account. Because it looks like a legitimate email from the President of the company, the Finance Assistant rushes to comply with the request. Unfortunately soon after the transfer is completed, the Financial Assistant discovers that the request was not truly from the President of the company. After IT gets involved, it is discovered that the email is "spoofed" to look like an email from the President. The company is out thousands of dollars and aside from reporting it to the Cybercrime division of the local police, nothing can really be done.

Solution: By implementing email security rules, ITS able to thwart future email spoofing attempts by identifying emails that are made to look like they are coming from an executive, but in fact are not. ITS also assists the client with the training of staff on how to identify possible phishing emails that contain malicious content.

Result: Client has peace of mind that employees will be on the lookout for potential malicious emails and if they are missed by the employee, the ITS tools will be working 24/7/365 to block any spoofed emails from even arriving to an employees inbox