# Email Security for Finance



Trustifi

We all remember the infamous Equifax breach where more than 44% of all Americans' financial information was exposed. The entire ordeal may end up costing Equifax more than $9.5 billion between assets and brand damage. The Equifax debacle is a prime example of why it is imperative that financial institutions secure themselves with the most advanced cybersecurity tools and solutions. Granted, your financial institution may not have been targeted by the Chinese government, but one day some bad actor might.

Anyone who has gone through the mortgage process will understand that a borrower provides a ton of personal and financial information to banks. If that information ends up in the wrong hands, someone who was attempting to better their living situation could have their life turned upside down. Many of these data breaches originate from email phishing schemes.

There are approximately 15 billion phishing emails sent per day; half of those target or impersonate financial institutions. The sheer volume of attacks indicates that an organization needs to beef up its email cybersecurity or be at risk of the wrath of hackers. If you think you can wait for this trend to die down in the financial industry, you are sadly mistaken.

The Belgian Bank Crelan sent €70 million overseas when the finance department was tricked into believing they were communicating with the CEO of the bank. If you believe that your employees are too smart or well-trained to fall for these schemes, there is a mountain of evidence that points to the opposite. Employees need an email cybersecurity solution that will lead them in the right direction the reputation of the entire business is on the line at all times.

During a data breach, your hard-earned name in the financial world will be dragged through the mud. Loyal, long-time customers will question why they work with your institution and may end up leaving you for your competitors. The only solution is to educate employees and implement an email cybersecurity solution that employees will actually incorporate.

This is precisely why Trustifi developed an email cybersecurity solution that is intuitive, comprehensive, and user friendly.

## Stopping Phishers in Their Tracks

No matter how well trained an employee is, they will be vulnerable to phishing schemes. Even IT employees -- who are typically the most well-versed in phishing scams in an organization -- are bound to make a mistake every now and then. Hackers now use images and PDFs, which were once considered safe, as new weapons in the phishing game. Thankfully, Trustifi's phishing detection system will improve your organization's defense against hackers.

Trustifi is able to protect employees from scammers in two different ways. A rating system will scan every incoming email and label it with a ranking that ranges from 'Authenticated' (the sender is who they say they are) to malicious, such as 'Impersonation Attack' or 'Spoofing Attack'. Simply reminding employees to take an extra step with artificial intelligence-powered software will make your organization more adept at fighting against hackers.

Trustifi also uses a behind-the-scenes inbound protection system that looks for malicious content in every incoming email. Administrators can create customized rules to guide the system how to act when certain types of threats are found, so that potentially harmful emails never make their way to a users' inboxes. Think of it as an AI-powered spam detector for malicious emails.

Phishing is not the only concern regarding email security. Many employees do not properly encrypt emails and attachments on outbound messages. Trustifi also has an easy-to-use solution that will ensure all emails that require encryption will be encrypted.

## Email Encryption Made Easy

Using Trustifi's email solution, administrators can create rules that automatically detect and encrypt messages that contain sensitive information. For the financial industry, these rules can detect PCI data or certain keywords, such as revenue or credit card information. When the system scans an outgoing email and finds a keyword or rule, the system will subsequently encrypt and lock the email without any input from the user.

This will ensure that sensitive data and attachments are not at risk before they reach their intended target. Our OCR (optical character recognition) technology will be able to recognize checks, credit cards, bank statements, and more. Your PCI data and reputation will not be at risk and your organization will be able to avoid hefty fines from government bodies.

Administrators can receive notifications when the system follows the rules in place and successfully encrypts an email with PCI data. Artificial intelligence has changed the game for email cybersecurity. Trustifi also has a multi-factor authentication system to identify the receiver of the email. These extra protections will help to ensure that your employees keep confidential and sensitive information safe from hackers.

**256-Bit AES Encryption**

NSA grade protection over your data and files

**Extra Security Features**

- One time access to files/emails
- Block access to print files
- Delete or edit messages after they have been sent

**Inbound Protection**

Stay protected from malicious links and files, viruses, phishing and spoofing attacks, ransomware attacks and even Spam.


**Multi-Factor Authentication**

on the recipient- You can choose to lock an email by adding a pin or a question that can only be unlocked by the intended recipient for an extra layer of protection

**No Log-in Portal or Account Necessary**

one click authenticate and decrypt allows your recipients to open your emails and also reply encrypted without ever having to sign up or login to anything

Contact Trustifi today to learn more about our comprehensive email security solutions specifically designed to protect financial organizations.

**www.trustifi.com**
1-844-235-0084
info@trustificorp.com