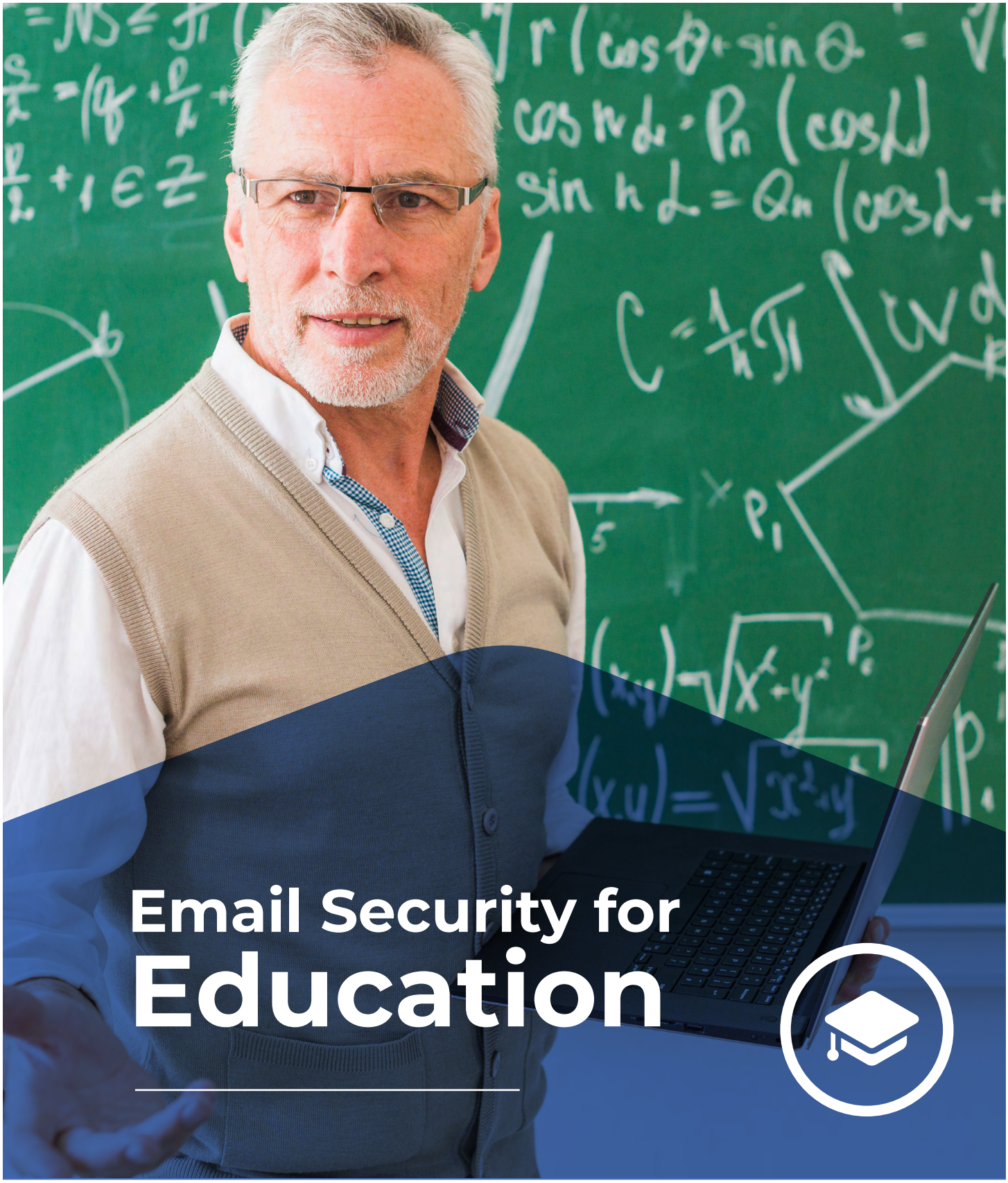


Email Security for Education

Trustifi

Education is the backbone of America; without it we would be left in the stone age. Students and teachers communicate heavily via email in the modern age as more classes have moved entirely online. Teachers and administrators constantly deal with student and family sensitive information - that provides ample opportunities for hackers to steal this data. Schools often have small budgets, especially in the IT department. This leaves schools in a very difficult position as they cannot properly defend themselves.

Researchers at universities also handle extremely valuable information that hackers would love to get their hands on. A recent report showed that Chinese hackers targeted more than 27 universities that were working on top secret military research. This is a huge worry for both universities and the military. Foreign interests look to exploit university weaknesses to gain key data for their own uses and undermine American interests.

The problem is that universities are set up in a way that makes it easy to collaborate with outside interests. That is amazing from a research perspective, but from a cybersecurity viewpoint, it leaves many vulnerability points. Professors and administrators can easily leak sensitive data unknowingly.

Between 2005 and 2013, there **were more than 550 data breaches** at U.S. universities. The number has increased over the past few years as hackers are more eager to target universities that do not have robust cybersecurity systems. Some universities are forced to pay off hackers, for example - one university in Germany had to pay **€300,000** after hackers infiltrated their systems.

Faculty are not the only risk factors in the education area. Students who are naive to hackers can also be easily phished and exploited. They often deal with sensitive data and they do not have access to the training that professors and administrators do. Cybersecurity education is an amazing tool, but schools and universities need a more effective way to reduce the number of data breaches. No matter how often you guide educators, phishing tactics almost always find a way to breach education institutions.

Stop Educators from Being Exposed to Phishing Schemes

The most seasoned educators may have the least computer experience and training. It is vital that education systems protect these individuals by creating the best defense for them. Phishers are using extremely complex methods to evade existing cybersecurity systems and intercept valuable data. Even IT executives with decades of experience can fall victim to these schemes.

Trustifi protects educators from phishers through two separate tools. The first tool is a rating system to help users identify a potentially malicious sender. The AI-powered system scans incoming emails and rates messages received from 'Authenticated' - the sender is who they say they are, to 'Impersonation Attack' - the sender is pretending to be someone else. Additionally, the system will alert the user if an email contains any malicious links or attachments. This tool will help end users identify hackers and take extra precaution and steps.

The other tool that Trustifi protects educators through its administrative inbound protection rules. School IT administrators can completely customize their rules to protect their users from a variety of phishing schemes. For example, phishers love to use grant applications to extract valuable data; administrators can create an inbound protection rule to ensure professors do not send valuable data to untrustworthy parties. Every single incoming email will be automatically scanned before it arrives in the recipient's inbox. If any sign of malicious activity is found, the email will end up in a separate quarantine area, instead of the user's inbox. By utilizing these two powerful tools, schools and universities can protect their faculty and students from emails phishing attacks.

Phishing is not the only aspect of security that educators have to worry about; encryption is another key part of cybersecurity. Many educators fail to appropriately encrypt their emails and attachments that contain sensitive data. Trustifi also has a useful tool to ensure that all educators will encrypt their emails.

Encrypting Sensitive Emails

A lack of email encryption can leave your education institution easily exposed to hacking incidents. Teaching an entire education workforce to properly encrypt emails can be an overwhelming task for even the most prestigious education institutions. That is precisely why Trustifi created a system that will ensure that every student and teacher will have properly encrypted emails, by utilizing AI technology to scan every outgoing email.

The artificial intelligence system identifies any potentially sensitive information in the email's body or attachments and will automatically encrypt and lock messages to remove the possibility of human error. Trustifi's system alerts users to encrypt their emails when sensitive information is entered. Users are protected from sending information to the wrong parties; Trustifi has a multi-factor authentication system to correctly ID the receiver of the email. The most convenient feature is that the recipient does not need to install software to identify themselves and are never forced to login or register to read their messages.

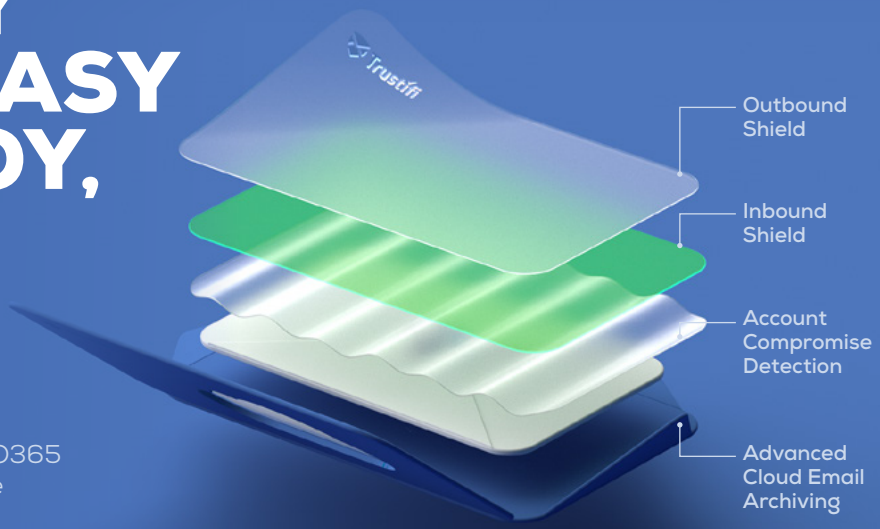
Trustifi ensures that your entire school or university will be protected from nefarious hackers. Regardless of size, whether you have 20 or 20,000 emails to protect, you will be up and running in under 20 minutes**.**

Trustifi

www.**trustifi**.com

Trustifi

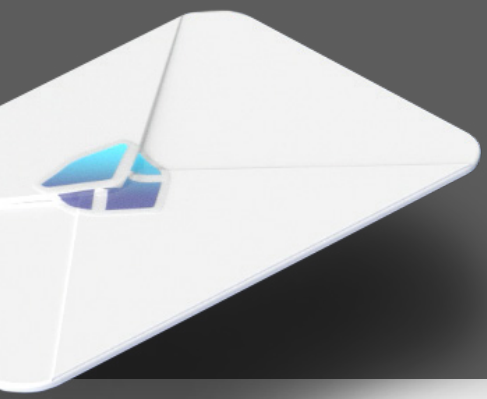
EMAIL SECURITY THAT IS EASY TO DEPLOY, MANAGE, AND USE



Easy integration with O365 and Google workspace

- Office 365
- Google Workspace

Customize a complete email security and compliance solution for your whole organization in minutes.



Outbound Shield

- Email Encryption and Recipient Multi Factor Authentication
- Data Loss Prevention and Email Data Exfiltration
- One-Click Compliance™

Inbound Shield

- AI engines to keep inbox clean
- Advanced Threat Protection
- Phishing and BEC Protection
- Stop SPAM and Gray Mail

Account Compromise Detection

- Instantaneously Identify Accounts that Have Been Compromised
- Automatically Block Access to Compromised Accounts

Advanced Cloud Email Archiving

- A cloud-based secure and convenient way to access emails
- Define controls and permissions to monitor and record user's activities
- Easily share data, cases and queries

Expert Insights ★★★★½ 4.8/5

Gartner peerinsights ★★★★★ 5/5

G2 ★★★★½ 4.8/5

Sales@trustificorp.com | +1 844-235-0084 | www.trustifi.com