# Practical Email Security Tips to Protect Valuable Business Data

A 2020 study reported that 306 billion emails were sent/received worldwide per day. An increasing number of those represent threats to valuable business data. Consider these practical email security tips as part of a multi-layered email security approach with the potential to save both you and your company a lot of time, embarrassment, and money.

With over half the world population using email, security professionals work diligently to thwart attacks while cyber-criminals increase in sophistication. However, email remains one of the primary attack vectors of cyber-criminals and a key area of vulnerability, hence the tips.

## 1. Separate Business and Personal Email

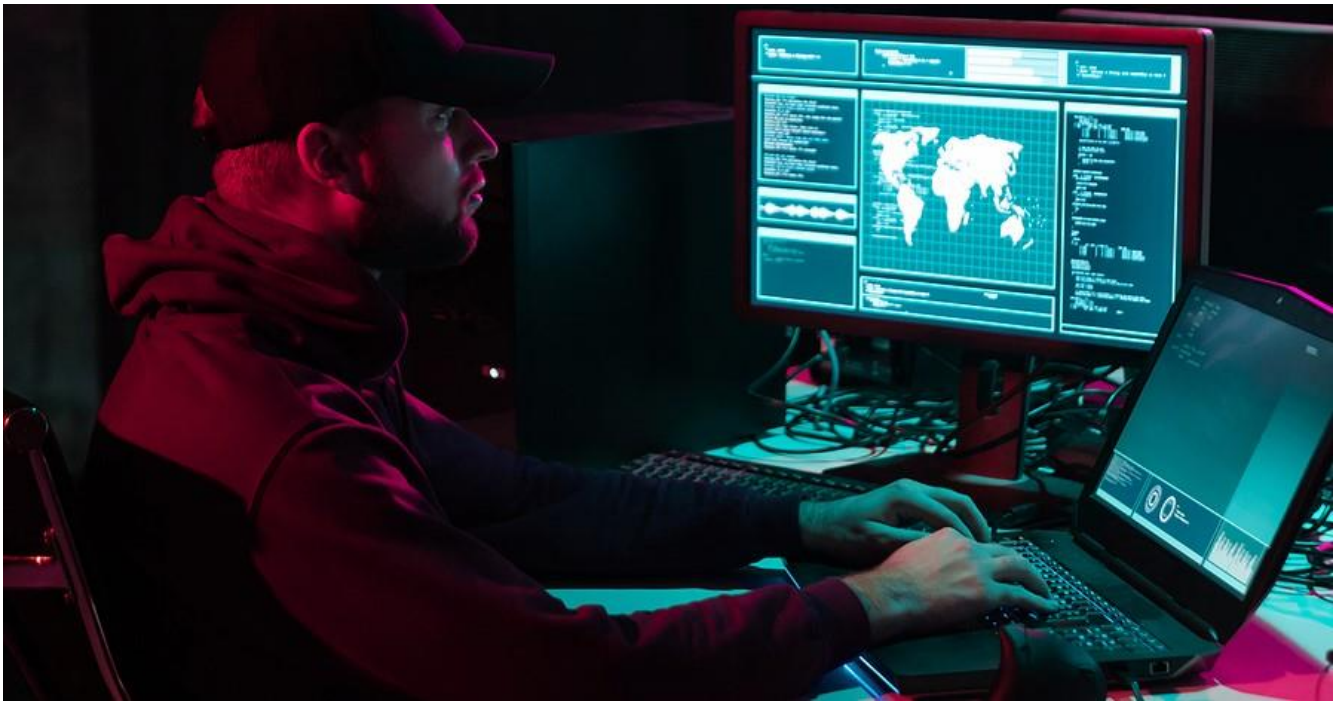
The corporate email that you send and receive belongs to the company. You have a responsibility to help protect it. To maintain your privacy and for the security of the organization, use your company email account only for business communication.

It's critical to maintain a separate email account for personal use. And make sure to establish unique passwords for each account. Sharing passwords between email accounts makes it easier for hackers to gain access to business data.

## 2. Share Files and Confidential Information Carefully

Despite what you learned in preschool; sharing is not always a good idea. When sharing files, think carefully before emailing that attachment or link. Ask yourself if the file must be shared and who really needs to see it. Check your shared folders often for information that should no longer be there.

Treat confidential information even more carefully. In a hurry, you might consider emailing account information to a vendor or your Social Security number to HR. Fight the urge. Sensitive personal or financial information should not be sent over un-encrypted email.



## 3. Always Be Suspicious of Phishing Schemes

Cyber criminals employ clever tactics to obtain personal information from workers by sending phishing emails that appear to be legitimate. For example, an email supposedly from your wireless company or a supplier may ask you to verify your credit card information or account password.

Red flags that may signal a phishing attempt:

- Hyperlinks – Take a few seconds to hover over a hyperlink to check the URL before you click the link. Be suspicious of miss-spellings in links that otherwise appear legitimate.
- Attachments – Absolutely do not open the file unless you are expecting the attachment, or if anything seems odd.
- Messages that ask for personal information - Often emails requesting Social Security numbers or passwords state that the sender is having trouble with your account. An email from a legitimate source will never ask for your password.
- Emails marked "Urgent".

- Poor grammar, spelling, or punctuation in the subject line or body.
- Use of financial terms in the subject like withdrawal, invoice, or statement.

No matter how convincing the email may sound, always be suspicious. And verify the source when you encounter something not quite right. Never just blindly follow the instructions in an email.

## 4. Verify the "To" Email Address

In addition to the tips above, slow down and take a moment to verify the target email address before you click Send. Frequently, senders overly rely on automatic address lookup. For example, a salesperson who has customers with similar names could easily send a confidential email to Robert Thompson that was intended for Thomas Robertson.

## Email Security Depends on You

Hopefully, your company has adopted email and file sharing best practices. In addition, comprehensive network security helps to protect sensitive company and customer information. However, the human element remains the weakest link in safeguarding valuable business data.

Indeed, secure email demands a knowledge of emerging email security threats and best practices. When used properly, email streamlines communication and serves as essential documentation. Messaging Architects works tirelessly to ensure the security of this valuable tool.