4 Common Sense Email Security Tips to Safeguard Vital Business Information

By Alexander Verlarde

Most of us spend a significant portion of our work day sending or responding to emails. In fact, a 2017 study reports that the number of emails sent and received each day, worldwide, exceeds 269 billion. As the number of emails grows, so do the number of email threats.

While hackers grow more proficient, security professionals work hard to keep pace. However, email remains a key area of vulnerability. Following a few basic email security tips can save both you and your company a great deal of frustration.

1. Be Aware of Common Phishing Schemes

Cyber criminals employ increasingly sophisticated tactics to gather personal information from users by sending phishing emails that appear to come from trusted sources. For instance, an email purportedly from your bank or a vendor with whom you have an account may ask you to verify your password or credit card information.

Red flags to watch out for include:

- Messages that ask for personal information, including Social Security numbers or passwords. Often these emails indicate that the supposed sender is having difficulties with your account. A legitimate source will never ask you for your password.
- Emails marked “Urgent”.
- Poor grammar or writing.
- Use of financial terms in the subject heading (Payment, Invoice, etc.)

- Hyperlinks – Always hover over a hyperlink to review the actual URL before you click the link. Look for miss-spellings in links that otherwise appear legitimate.
- Attachments – If you were not expecting an attachment, or if anything appears less than normal, do not open the file.

Never just blindly follow the instructions in an email, no matter how convincing the writer may sound. Always be suspicious and verify the source when you encounter something unusual.

2. Keep Business and Personal Email Separate

Remember that your corporate email does not belong to you. It belongs to the corporation. For your own privacy and for the security of the company, reserve your corporate email account for business communication.

Keep a separate email account for personal use, and make sure to create a unique password for each account. Re-using passwords between accounts leaves you vulnerable to hackers.

3. Share Wisely

Despite what your mom taught you, sharing is not always the best idea. When it comes to files, think carefully before you email that link. Share only the information that needs to be shared and only with the people who need to use it. Review your shared folders regularly. Information that was valid last month may no longer be valid today.

Apply even greater caution with confidential information. When you are pressed for time, you may be tempted to email credit card information to a vendor or your Social Security number to Human Resources. Resist the temptation. Un-encrypted email is not the place for sensitive personal or financial information.

4. Double-check the Target Email Address

In conjunction with wise sharing, take a minute to slow down and verify the email address before you click Send. All too often, users rely too much on fast lookup. Take, for example, an associate who has customers with similar names. It would be easy to accidentally send a confidential email to Mary Sanderson that was intended instead for Marion Sanders.

Email Security Depends on You

Hopefully, your company has invested in [multi-layer email security](). Comprehensive [network security]() is a must for protecting vital corporate and customer data. However, the human element remains the most unpredictable factor in safeguarding information assets.

When properly used, email streamlines communication and provides essential documentation. Take the time to educate yourself about emerging email security threats and implement best practices to ensure that you are getting the most out of a valuable tool.

Alexander Verlarde joined the team at Messaging Architects (formerly Netmail, and now a division of eMazzanti Technologies) in 2006. Currently, he works as a Professional Services Technician, focusing primarily on implementations. He particularly enjoys the challenge of solving problems and helping systems run smoothly.