



The MERIT Quick Guides are a series of step-by-step instructions to help you harness the power of technology.



When you typically send an email, that message is accessible by you, the recipient, and whoever has access to the email servers. That might seem like security enough. After all, without your Outlook login, how would anyone be able to read your email?

Unfortunately, hackers don't need your Outlook password or 2FA code in order to intercept your email. That's because regular email is sent in plain text: If hackers break into your email server, your messages will appear as they do for you and your recipients. That's bad in general, but even worse if you send sensitive information over email.

One simple way to protect your emails in Outlook is to encrypt them. When you encrypt an email, or any data for that matter, it converts the email from plain text into "ciphertext," a scrambled mess of numbers, letters, and characters no person would be able to interpret. If someone were to break into your servers, they'd be met with this incomprehensible data, and would have no way of knowing whether the message contained critical banking information, or a simple meeting request.

While we can't read ciphertext ourselves, it isn't random. An algorithm is responsible for converting plain text into ciphertext, and that algorithm can convert it back when need be. The only way to convert your ciphertext back into plain text, though, is to have the key necessary to do so.

In this case, the key for decrypting your ciphertext emails is your Microsoft Account password and 2FA. Whether you send the encrypted message yourself, or you receive an encrypted message, your Microsoft Account can unscramble the data to present the message in plain text as originally written. If you send an encrypted message to someone without Outlook, their email account's password will be their key.

Getting in the habit of encrypting your emails helps to ensure hackers and other nefarious users cannot access, read, or steal your sensitive data, and is an important tool in your cybersecurity arsenal.

About MERIT 2.0

MERIT was founded in 1983 and was re-branded in 2020 as MERIT 2.0. Our Mission Statement is *To educate every worker at every client and provide them the technology to improve.*

Quick Guides copyright by MERIT 2.0 and may not be copied or redistributed without permission.

How to Contact MERIT 2.0

SERVICE/REPAIRS/HELPDESK:
service@meritsolutions.net
or call 757-420-5150

www.meritsolutions.net

MARKETING:
marketing@meritsolutions.net
or call 757-420-5150 x7007