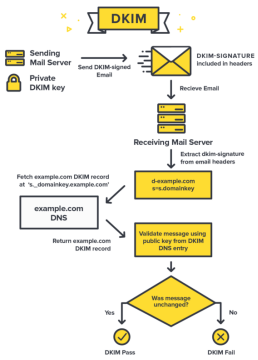
GainPlus included DKIM for outgoing emails

GainPlus has recently included DKIM on our mail servers so that mail sent from our Leave (and soon to come Payroll) servers will be signed by keys managed by our own PKI certificates. What does this mean to users?
Well, perhaps not a lot will be seen by users.

Techopedia explains DomainKeys Identified Mail (DKIM)



“The digital signature used in DKIM provides an additional way to tell whether an email is forged. Spammers often forge headers or other aspects of an email to make the message look like it comes from a legitimate source. DKIM uses domain information to authenticate the email’s origin.
Experts point out that DKIM will not necessarily eliminate spam, but it will help to ensure that a legitimate source stands behind a message and is responsible for it. It’s important to note that a message can be validated at various points in its trajectory, and that the specifics of this authentication method may vary according to service providers.”

User’s mail servers need to be able to understand DKIM, but many modern mail servers do, including O365 and Google mail servers.

Security is important to GainPlus and we go the extra mile to protect our client’s data, whether on our servers or in transit.