GTMailPlus.Anti-Phishing

Comprehensive protection against email social engineering attacks

GTMaritime's latest security addition **GTMailPlus.Anti-Phishing** gives you comprehensive protection against the latest type of email social engineering attacks. Created to help protect your business from becoming another phishing statistic. Anti-Phishing runs 8 individual checks, developed to identify potential phishing emails.

Why do I need Anti-Phishing?

Phishing is a type of social engineering attack often used to steal data, including login credentials and bank details. It happens when an attacker, masquerading as a trusted entity, tricks a victim into opening an email. The recipient is then tricked into opening a malicious link or responding with sensitive information, which can lead to the installation of malware, the freezing of the system or the revealing of sensitive information with potentially devastating results.

Anti-Phishing allows customers to choose from 4 options to highlight potential phishing threats, helping to protect against attacks, potentially saving you millions.

> **156 million phishing emails** are sent out every day
>
> UKFast, 2019

> **90% of business** have suffered a data breach from a **maliciously crafted email**
>
> UKFast, 2019

GTMARITIME
data · optimised · secured · delivered

6,000+ vessels worldwide trust GTMaritime with their communication solutions

500+ businesses worldwide connected

Learn more about **GTMailPlus.Anti-Phishing**. Speak to our sales team today.

E: sales@gtmaritime.com **T**: +44 (0) 1925 818918

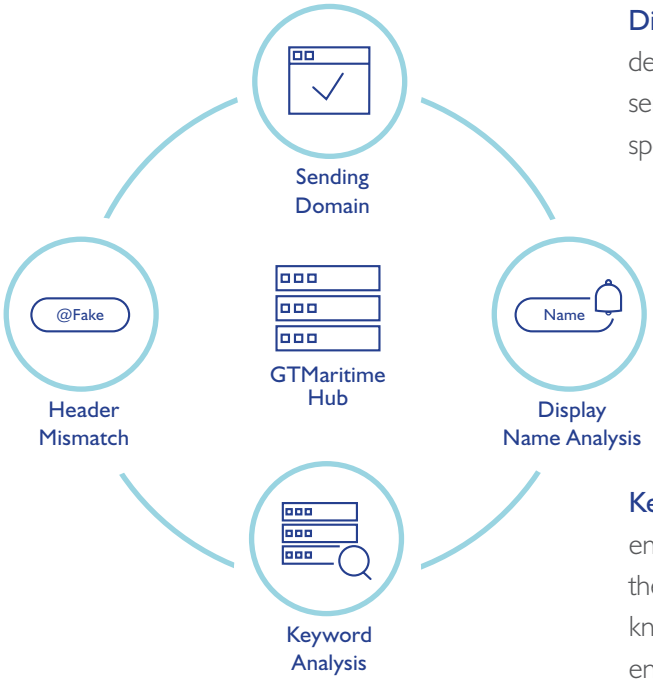
Benefits of GTMailPlus.Anti-Phishing

- ✔ **End user protection** - tags potentially suspicious emails
- ✔ **Complete control** - administrative ability to release quarantined content or block future instances of quarantined mail
- ✔ **Choice of 4 alerting mechanisms** - option to route emails directly to quarantine, allow emails to be delivered with no action or chose from 2 options to highlight a suspected phishing email
- ✔ **Keyword analysis** - uses a targeted threat database to identify suspicious terms
- ✔ **Observes newly created domains** - protects against newly created domains used to attack
- ✔ **Spoofing protection** - detects spoofing attempts containing display name and reply to mismatch

How GTMailPlus.Anti-Phishing works

GTMailPlus.Anti-Phishing protection examines a number of key indicators whilst examining email content including:

Sending domain – validates the age of registration and determines if the sending domain is genuine. Monitoring closely matched domain names to a true corporate domain



Display name analysis – determines whether the sender is attempting to spoof an internal sender

Header mismatch – determines whether the sender is hiding their real email address

Keyword analysis – emails are examined against the threat database for known attack phrases to ensure authenticity of content

If detected as suspicious the email will be tagged for quarantine. Which can be closely monitored through reporting and control using the **GTMaritime Dashboard**.

Learn more about **GTMailPlus.Anti-Phishing**. Speak to our sales team today.

E: sales@gtmaritime.com **T**: +44 (0) 1925 818918