GTMailPlus. Anti-Phishing

Comprehensive protection against email social engineering attacks

> **91% of cyberattacks start with a phishing email.**
>
> **Phishme, 2016**

GTMaritime's latest security addition 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.

More than **4,000 ransomware attacks** have **occurred every day** since the beginning of 2016. That's a **300% increase** over 2015, where 1,000 ransomware attacks were seen per day.

Computer Crime and Intellectual Property Section (CCIPS), 2016

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. An attack can lead to devastating results. For individuals, this includes unauthorized purchases, the stealing of funds, or identify theft. GTMailPlus.Anti-Phishing solution protects and prevents against this, potentially saving you millions.

GTMaritime

5,000+ vessels worldwide trust GTMaritime with their communication solutions

500+ businesses worldwide connected

GTMARITIME
SECURING ESSENTIAL COMMUNICATIONS

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

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

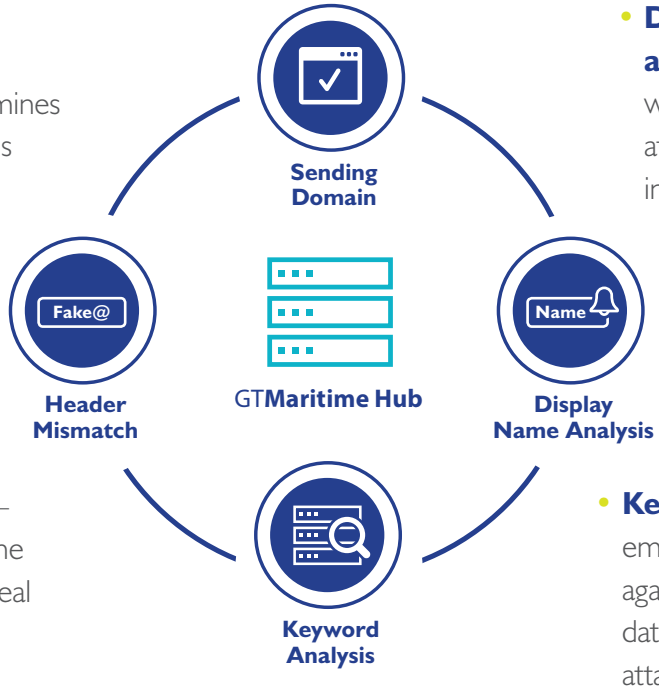
Benefits of Anti-Phishing

- ✔ **End user protection** - tags potentially suspicious emails
- ✔ **Complete control** - administrative ability to release quarantined content or block future instances of quarantined mail
- ✔ **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 it 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
- **Header mismatch** – determines whether the sender is hiding their real email address
- **Display name analysis** – determines whether the sender is attempting to spoof an internal sender
- **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 GT**Maritime Dashboard**.

GTMARITIME
SECURING ESSENTIAL COMMUNICATIONS

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

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