IN 1427 – IMCA Security Bulletin 01/19

Information Note Published on **22 January 2019**

The IMCA Security Committee is determined to raise awareness of security issues that can potentially harm member companies. Information provided in this regular Security Bulletin is intended to be used by Members to either directly pass on to employees or use the material it contains as part of an existing company security awareness programme.

1. Cyber security

The *Be Cyber Aware at Sea* web site is recognised as a useful tool to assist in raising awareness. Each of the first eight IMCA security bulletins will refer the reader to one of the *Be Cyber Aware at Sea* poster and video campaigns; this bulletin it is, *Watch where you surf*.

IMCA Contact:

Nicholas Hough
Consultant – Safety & Security

Original IMCA author:

Richard Purser
Technical Adviser – Marine

Committees:

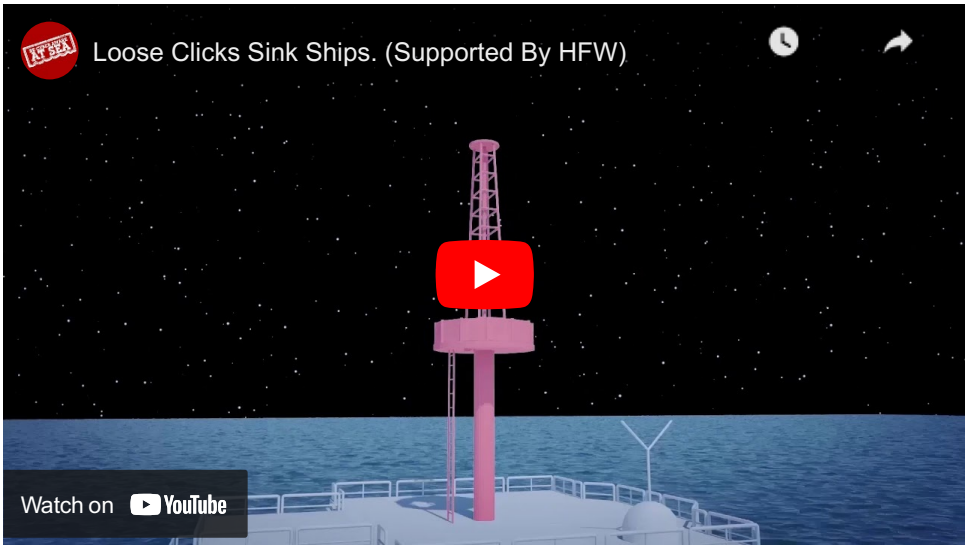
HSS - Security

Tags:

#Health, Safety & Security #Security


BE CYBER AWARE AT SEA
LOOSE CLICKS
SINK SHIPS!
Be wary of pop-ups, emails and websites asking for sensitive information.

Video


Loose Clicks Sink Ships. (Supported By HFW)
Watch on YouTube

2. Traditional security

Links to recent security related information:

- Combined Maritime Forces Industry Releasable Threat Assessment
- NATO MARCOM Monthly Newsletter (dated January 2019)
- Member analysis of US Naval Deployment to the Gulf

The IMCA HSSE Security committee is pleased to endorse and support the following guidance for the benefit of members:

Each Guidance Document is unique and supports the overall aim of being prepared and taking mitigating measures. In relation to cyber security, this will eventually become a compliance issue. All companies will be required to conduct a Cyber Security Risk Assessment to demonstrate how to mitigate and deal with the threat of a cyber security attack

BMP5

The 5th edition, issued June 2018, is an extremely useful and comprehensive guidance. It introduces effective measures for the protection of crew, vessels and cargo while transiting the Red Sea, the Gulf of Aden, the Indian Ocean and the Arabian Sea. The new edition supersedes BMP4.

BMP5

Global Counter Piracy Guidance for Companies, Masters, and Seafarers

This Guidance will help companies and mariners prepare for and mitigate against piracy wherever it occurs. The guidance is applicable for all ship-types and complements regional guidance (BMP5) on piracy and Maritime Security.

Global Counter Piracy Guidance for Companies, Masters, and Seafarers

Guidelines to harden vessels (OCIMF)

This new guidance, released in July 2018, from OCIMF recommends a layered defence methodology for hardening vessels to help prevent unauthorised boarding. The Guidance also recommends using a Vessel Hardening Plan (included in the document) to help ensure vessels are prepared for operations in areas of increased security. Although the focus is on vessels when underway, measures are also examined for vessels at anchor and alongside.

Guidelines to harden vessels (OCIMF)

General cyber security guidance for vessel/ship-owners

This third edition, published on 7 December 2018, provides additional information to assist shipping companies carry out risk assessments and include measures in their safety management systems to protect ships from cyber-incidents. A new dedicated annex provides measures that all companies should consider implementing to address cyber risk management in an approved Safety Management System.

General cyber security guidance for vessel/ship-owners – IMO

Guidance on security threat risk assessment procedures (IMCA M236)

This guidance is aimed at the process of identifying security threats and determining vulnerability of company assets, including its employees, to the threats identified, so that security procedures, resources and measures can be allocated most effectively and efficiently.

IMCA M236

HSS Security

Technical Library