THE HUMAN FIREWALL:

SECURING THE CREW, SAFEGUARDING THE SHIP

IN THE COMPLEX OPERATIONAL ENVIRONMENT OF A VESSEL, THE INTEGRITY OF YOUR DIGITAL SYSTEMS IS AS CRUCIAL AS THE SEAWORTHINESS OF THE HULL. WHILE SOPHISTICATED TECHNOLOGY ACTS AS A SHIELD, THE SINGLE MOST CRITICAL VULNERABILITY IS OFTEN FOUND NOT IN THE HARDWARE OR SOFTWARE, BUT WITH THE PEOPLE OPERATING IT. AN ESTIMATED 74% OF ALL CYBER BREACHES START BECAUSE OF THE HUMAN ELEMENT.[1] THIS STAGGERING FIGURE UNDERSCORES A SIMPLE TRUTH, THAT THE MOST VULNERABLE POINT IN CYBER SECURITY IS OFTEN THE PERSON AT THE KEYBOARD.

ROB PRESTON, SENIOR TECHNICAL SALES ENGINEER, GTMARITIME

GTMaritime, providers of secure communication software for remote workers, ran controlled phishing simulations across a variety of vessels. The results were stark: Industry benchmarks suggest that phishing test failure rates typically fall between 2–5%[2]. GTMaritime results revealed 15% of maritime users clicked malicious links, with 7% submitting personal data.

Cyber security therefore cannot solely be the responsibility of the shore-based IT department, it must be understood and adopted as a shared responsibility by everyone onboard. By fostering a vigilant, security aware mindset, every crew member can actively contribute to the vessel's digital safety.

To be an effective human firewall, you must first understand how criminals exploit psychology, trust, curiosity and urgency, to bypass technical controls

PHISHING: THE DECEPTIVE LURE

The most common tactic remains phishing, a fraudulent attempt to acquire sensitive information such as login credentials, passwords or financial details. Attackers impersonate a trustworthy entity, casting a wide net commonly via email or text message hoping to trick the recipient into clicking a malicious link or downloading an infected file.

Your defence against phishing requires caution. Always verify the sender's email address and check for subtle misspellings in the domain. Treat unexpected or demanding messages with suspicion: never click links or open attachments. Forward suspicious emails immediately to your relevant IT manager for verification. Criminals deliberately create a sense of urgency, a missed invoice, a security alert to bypass rational thought. Resist this impulse and always think before you click.

MALWARE: THE SILENT INTRUDER

Malware is malicious software designed to disrupt, damage or gain unauthorised access to a computer system. This category includes viruses, spyware and other code designed for destruction or espionage.

Malware often spreads through seemingly innocent means. For example, USB devices can be a risk because they can be pre-loaded with malware and infect systems the moment they are connected. An infected USB device found on the floor, could be a deliberate attempt for infection. The rule is simple; only use company approved and scanned USB devices that are essential for specific tasks. Do not connect any personal or unknown devices into a vessel's network, particularly those connected to operational technology or critical bridge systems.

RANSOMWARE: THE OPERATIONAL HOSTAGE

A highly disruptive form of malware is ransomware, which works by encrypting computer files, locking out the legitimate user and demanding a ransom payment for recovery.

If a vessel's systems are affected, the consequences can be severe. Navigation charts, planned routes, engineering logs and communication records could be rendered inaccessible. This can lead to full operational paralysis, delays, or loss of control over key systems. Paying the ransom is never a guarantee of recovery and simply funds further criminal activity. Prevention is the only reliable cure. The key preventative measure is ensuring regular isolated backups of all essential data are maintained, allowing the ship to restore systems without giving in to criminal demands. Alongside your constant alertness against phishing and malware, this dual approach ensures strong cyber resilience.

SOCIAL ENGINEERING AND MEDIA RISK

Beyond technical exploits, social engineering is the psychological manipulation of people into performing actions or divulging confidential information. This tactic leverages human trust through impersonation or false authority. An attacker might telephone the vessel claiming to be an engineer needing an urgent password to fix a critical connection. Always treat unsolicited requests for sensitive information with extreme suspicion and verify them through a prearranged independent channel.

Even your personal habits could compromise the vessel's security. Social media accounts provide attackers with valuable intelligence they can use to craft believable attacks. How you portray yourself online can unintentionally put you at risk. A personal post showing the vessel's cargo in the background, or a seemingly harmless check in with your real time location can unintentionally expose operational details that aid an attacker. Maintain high privacy settings, avoid sharing specific work details, and treat all information about the ship and its operations as commercially sensitive.

FOSTERING A CULTURE OF TRUST AND ACTION

The final layer of defence is a well-prepared crew. The goal is to foster a culture of cyber trust onboard. Crew must feel safe reporting anything suspicious without fear of reprisal. Incident drills, like fire or safety exercises, should rehearse reporting, isolation and communication with shore teams.

Everyone must feel comfortable and safe to speak up without fear of repercussion when they spot anything suspicious. If you see something, you must know immediately who to report to and how to safely initiate a response.

In an active incident, speed is important, but the wrong action could be worse to operations. The priority is containment which is crucial to prevent the spread of malware or ransomware across the network. Isolating a compromised device is necessary, but you must do so with operational impact in mind. You do not want to unintentionally disconnect a navigation system while isolating an infected crew computer which operates in a segmented part of the network.

The solution is a tailored incident response plan to your environment and operational needs. This should be treated like fire safety or health and safety procedures. Do regular drills that practise reporting, isolating systems and communicating with shore side teams. This preparation ensures crew members know who to notify, how to safely isolate a system and what information to immediately capture about the incident.

To achieve this state of readiness, organisations are increasingly turning to dedicated solutions, using human risk management platforms to turn every crew member into the proficient, vigilant human firewall the maritime industry now depends upon.

CONCLUSION

The next great maritime incident may not be caused by a mechanical failure or an act of piracy, but by the single, innocent click of an unaware crew member.

The digital security of a vessel is a continuous, collective challenge. As technology progresses, so too does the sophistication of the attackers. The integrity of global trade, the safety of the crew and the continuity of the voyage depend on more than just high-tech solutions. Success rests on the vigilance of every seafarer.

1. Information Commissioner's Office, "Learning from the Mistakes of Others – A Retrospective Review: Errors," accessed October 20 2025, https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/learning-from-the-mistakes-of-others-a-retrospective-review/.
2. Your DMARC. "Phishing Simulation Benchmarks: What's Normal in 2025?" Support Center. Updated over 6 months ago. Accessed October 20, 2025. https://support.yourdmarc.com/en/articles/11069886-phishing-simulation-benchmarks-what-s-normal-in-2025.