Secure State Cyber: Cyber risks on board passenger vessels

Secure State Cyber have been specialising in information and cyber security since 2005. Their mission is to create security for everyone within the digital space. Their consultants are specialists in information security and come from a diverse range of academic backgrounds, including civil engineering, computer systems, law with specialty integrity protection, cognitive science, civil economics and computer networking.

In collaboration with Secure State Cyber, the Club will be releasing a series of short FAQ articles identifying common cyber risks on board and what actions Members can take to ensure the security of their vessels. The first article focuses on passenger vessels and the cyber risks associated with on board Wi-Fi and passenger devices.

Should passenger vessel owners and operators allow availability of Wi-Fi to all passengers?

These days passenger vessels are almost always expected to provide Wi-Fi for guests but there are associated risks in allowing passengers to use publicly available Wi-Fi on board. It is strongly recommended that passengers are offered a guest Wi-Fi network, with client isolation (this stops a user's device from detecting and sending data to other devices on the same network). It is also recommended that this network be kept completely separate from the Wi-Fi network responsible for controlling the ship's vital navigation and communication systems including that for on board administrative tasks.

There should be clearly established controls that prevent devices accessing both the public Wi-Fi and the restricted systems. Further network segregation should also be implemented for the administrative network and the critical ship systems such as the Industrial Control System (ICS). This also extends to include the devices that can connect to critical systems on board.

No passenger or crewmember should be able to use the same device to access both the public Wi-Fi and the restricted systems. Public Wi-Fi is often unsecure and uncontrolled and the vessel's critical systems should never be put at risk by having contact with it, directly or indirectly.

Are there specific signs that passengers should be cautious about when using the vessel's Wi-Fi?

Passengers should by mindful of:

- Networks that are spelt incorrectly, or that do not have a secondary measure to access the service. Members providing free Wi-Fi should ensure that passengers know they require a password to access the service and that they are aware of the correct Service Set IDentifier (SSID) or Wi-Fi network name on which to connect.
- Using a Virtual Private Network (VPN) when using public Wi-Fi. Passengers should be careful and take precautions when using networks that are not controlled, where the network is open, and the users are not separated from each other. Public Wi-Fi should only be used for general browsing.
- Ensuring that web browsers (Chrome, Safari, Firefox or Internet Explorer) are kept updated. Most systems update automatically, however this is not always the case, especially if browsers are not closed/shut down.
- Accessing websites that are secured with https (s stands for secure). Do not ignore certificate errors that may pop-up before accessing a site as these could be an indication that the site is a malicious copy, or someone is capturing and replaying the traffic to the user. Ensure the web address entered is correct and not misspelt. Misspelt addresses can be an indication of a typo squatting attack, where malicious sites copy and have similar names to a legitimate website.

Efforts to draw attention to this guidance in the form of posters and cyber safety notices around the vessel should be made, so that passengers are readily aware of these precautions.

What should passengers do if they think they've been hacked?

Report it to a crewmember who can escalate the issue to the captain for further investigation into the suspected event. Members should ensure that the necessary resources are available to respond to and investigate any suspected events.

Should mobile phone / USB charge points be made accessible to passengers?

A simple principle to be kept in mind is that if a physical connection to a device is possible, then the contents of that device can be accessed. However, there are exceptions and it is recommended that Members only offer Dedicated Charging Ports (DCPs) / USB ports to passengers for charging their devices.

DCPs provide power via USB ports without any possibility of data transfer. DCPs will provide up to 1.5 A and 5 V, which is more than enough for charging mobile phones or tablets. There is also an added benefit by only offering DCP charging stations to passengers, their privacy can be guaranteed, and the security of their devices can remain uncompromised. By offering anything other than DCPs for charging, Members and passengers should assume that data transfer is possible from their devices. Members can provide a reasonable guarantee of security by performing cybersecurity audits or having their systems regularly assessed for security faults or vulnerabilities themselves. Having a third party assess security and provide feedback is a useful way of ensuring the passengers' and vessel's security.