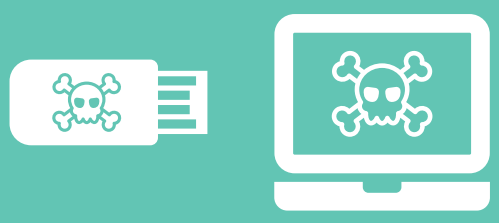
CYBER SECURITY ONBOARD SHIPS

Cyber security is everybody's responsibility.
The information provided here gives advice on how your actions can help to avoid cyber incidents.

POTENTIAL THREATS



KEEP UNAUTHORISED SOFTWARE AWAY FROM SHIP SYSTEMS!

- Scan for viruses and malware before you connect authorised USB memory sticks to onboard OT and other networked systems.
- Personal laptops, tablets, USB memory sticks or phones must not be connected to on board operational systems.

INCIDENTS

BE PREPARED!

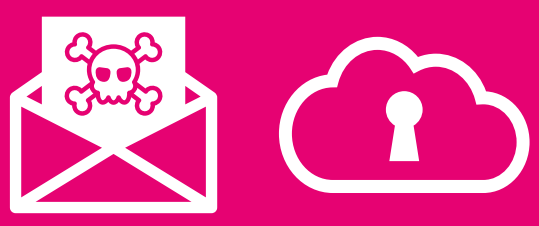
- Keep your crew and any passengers safe – train for what to do if important OT systems do not work.
- Know where to get IT and OT assistance.
- Report suspicious or unusual problems experienced on IT and OT systems.

PASSWORD PROTECTION

BE IN CONTROL!

- Use new passwords every time you sign on to a ship.
- Choose complex or randomly generated passwords with num6er5s, $ymbo!s, and some CaPiTaL letters. Be careful, you have to be able to remember them.
- Keep your user names and passwords to yourself.
- Update default user passwords and delete passwords of colleagues who have left the ship.

SUSPICIOUS ACTIVITY



BE VIGILANT WHEN YOU COMMUNICATE!

- Only open emails or open attachments from senders that you know and trust.
- Know what to do with suspicious emails.
- Think before you share information on social media or personal email about your company, job, ship or the crew.

INTERNATIONAL CHAMBER OF SHIPPING

BIMCO

MPA SINGAPORE

OT: Operational Technology is the systems which are used to operate the ship.

IT: Information Technology is the systems used for office work, email and web-browsing.