Cyber Security — study guide

Cyber-crime attacks people first, not machines — which is why your habits are the ship's first line of defence. This guide covers the threats, the everyday precautions and the signs of a phishing approach.[1]

The threat and the response

To combat cyber-crime, many countries and international organisations have implemented individual data rights and created laws enabling data-protection standards, and have created and sponsored best-practice standards. Your company depends on you to be the first line of defence, and your online habits matter.

Everyday precautions

- **Turn off Bluetooth** when you don't intend to use it — it is a potential gateway for cyber-criminals into your smartphone.
- **Use a strong password and never share it.**
- Don't open an attachment unless you know who it is from and you are expecting the file.
- Lower the risk of an e-mail virus by **knowing who sent you an e-mail and why**.
- Remember that posting personal information on social media **does** compromise your cyber-security.
- A smartphone can get viruses just like a computer.
- Never having had a problem downloading free music and movies does **not** make it safe.

Phishing and personal approaches

A common way for cyber-criminals to make a personal approach is **spear phishing** — a targeted message crafted for you. A reputable business will **not** ask for your personal information or credit-card details via e-mail. The single most effective upgrade is attitude: move from "It won't happen to me" to "I'm a potential target".

Safer practice

Generally, using **your smartphone as a mobile hotspot** is safer than joining unknown Wi-Fi networks. Treat unexpected links, attachments and requests as suspect until verified.

Key facts to remember

- You are the first line of defence; your online habits count.
- Turn off Bluetooth when unused; use a strong password and never share it.
- Don't open unexpected attachments; know who sent an e-mail and why.
- Spear phishing is the common personal approach.

© 2026 maritimetest.com · free study guide

- Posting personal information online compromises your security.
- A smartphone can catch viruses; free downloads being "fine so far" proves nothing.
- A reputable business won't ask for personal or card details by e-mail; use your phone as a hotspot.

Sources

1. IMO Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3) — shipboard cyber risk management, with the ISM Code (SOLAS Chapter IX).