Cyber Security – Onboard

David Patraiko, FNI
Director of Projects
The Nautical Institute

25 April 2016
Digital Ship – Athens

About us

The Nautical Institute is an international representative body for maritime professionals involved in the control of sea-going ships. We provide a wide range of services to enhance the professional standing and knowledge of members who are drawn from all sectors of the maritime world.

www.nautinst.org

Watch... An introduction to The Nautical Institute

www.youtube.com/user/TheNauticalInstitute

Cyber Security

September 2014 www.nautinst.org

Seaways

The International Journal of The Nautical Institute

Navigational audits
Making them count p5-8

GNSS alert
Glonass failure analysed p12

Compass adjustment
Allowing for error p15

Mind that cable
Anchoring trials p24

Cybersecurity
Confronting the threat p9-11

The Nautical Institute

September 2014

THE NAVIGATOR

Inspiring professionalism in marine navigators

FREE

Cyber Security

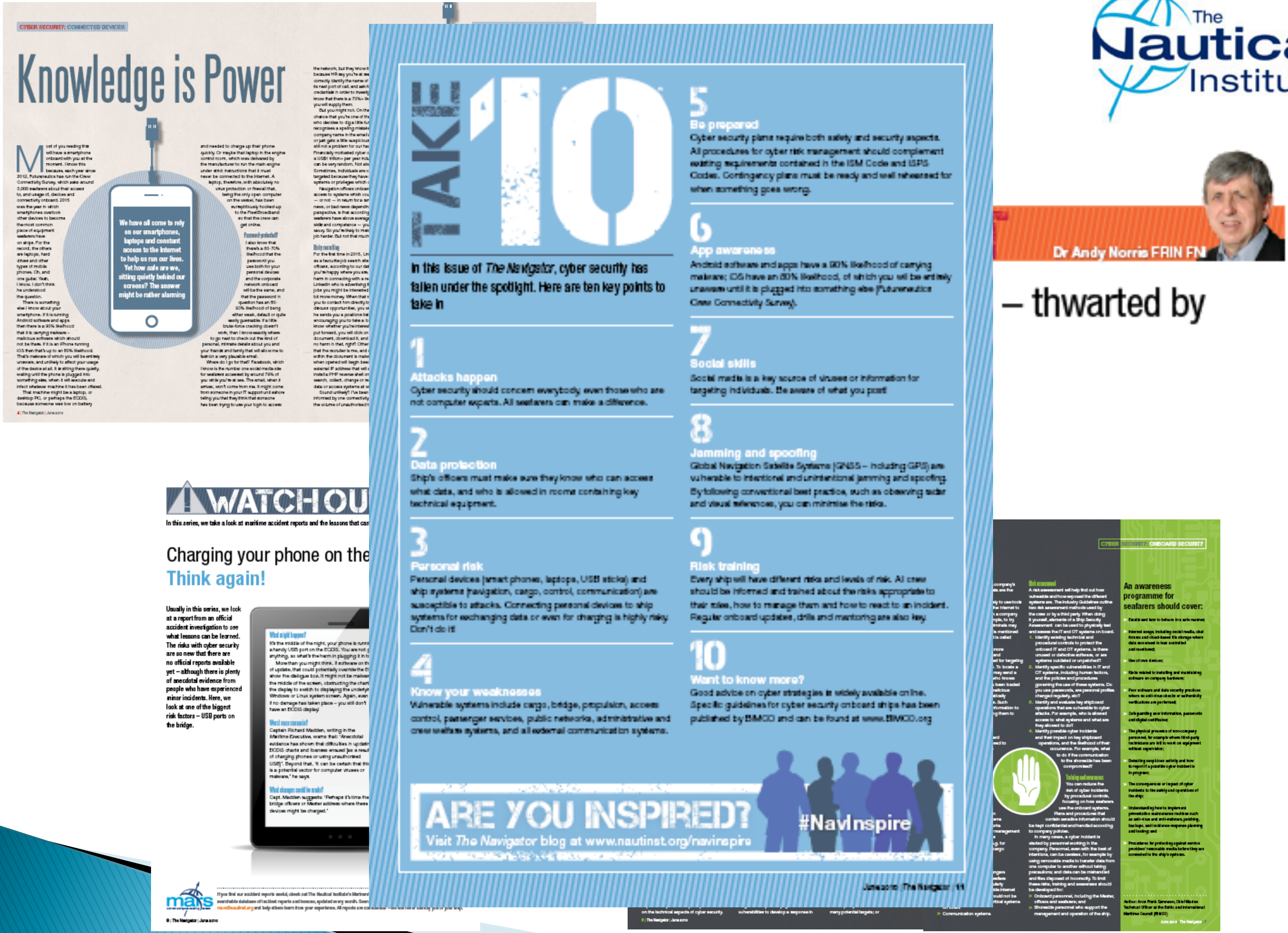
Cyber hygiene and the use of ICT on board

The Nautical Institute

A free publication by The Nautical Institute in association with the Royal Institute of Navigation

June 2016 – FREE

The Nautical Institute



CYBER SECURITY: CONNECTED DEVICES

Knowledge is Power

We have all come to rely on our smartphones, laptops and constant access to the Internet to help us run our lives. Yet how safe are we, sitting quietly behind our screens? The answer might be rather alarming

TAKE 10

In this issue of *The Navigator*, cyber security has fallen under the spotlight. Here are ten key points to take in

1 Attacks happen
Cyber security should concern everybody, even those who are not computer experts. All seafarers can make a difference.

2 Data protection
Ship's officers must make sure they know who can access what data, and who is allowed in rooms containing key technical equipment.

3 Personal risk
Personal devices (smart phones, laptops, USB sticks) and ship systems (navigation, cargo, control, communication) are susceptible to attacks. Connecting personal devices to ship systems for exchanging data or even for charging is highly risky. Don't do it!

4 Know your weaknesses
Vulnerable systems include cargo, bridge, propulsion, access control, passenger services, public networks, administrative and crew welfare systems, and all external communication systems.

5 Be prepared
Cyber security plans require both safety and security aspects. All procedures for cyber risk management should complement existing requirements contained in the ISM Code and ISPS Codes. Contingency plans must be ready and well rehearsed for when something goes wrong.

6 App awareness
Android software and apps have a 90% likelihood of carrying malware; iOS have an 80% likelihood, of which you will be entirely unaware until it is plugged into something else (Futurenautics Crew Connectivity Survey).

7 Social skills
Social media is a key source of viruses or information for targeting individuals. Be aware of what you post

8 Jamming and spoofing
Global Navigation Satellite Systems (GNSS – including GPS) are vulnerable to intentional and unintentional jamming and spoofing. By following conventional best practice, such as observing radar and visual references, you can minimise the risks.

9 Risk training
Every ship will have different risks and levels of risk. All crew should be informed and trained about the risks appropriate to their roles, how to manage them and how to react to an incident. Regular onboard updates, drills and mentoring are also key.

10 Want to know more?
Good advice on cyber strategies is widely available online. Specific guidelines for cyber security onboard ships has been published by BIMCO and can be found at www.BIMCO.org

ARE YOU INSPIRED?
Visit *The Navigator* blog at www.nautinst.org/navinspire
#NavInspire

June 2016 | The Navigator | 11

WATCHOUT

In this series, we take a look at maritime accident reports and the lessons that can

Charging your phone on the
Think again!

Usually in this series, we look at a report from an official accident investigation to see what lessons can be learned. The risks with cyber security are so new that there are no official reports available yet – although there is plenty of anecdotal evidence from people who have experienced minor incidents. Here, we look at one of the biggest risk factors – USB ports on the bridge.

What might happen?
It's the middle of the night, your phone is runni
a handy USB port on the ECDIS. You are not g
anything, so what's the harm in plugging it in to

More than you might think. If software on th
of update, that could potentially override the E
show the dialogue box. It might not be malwar
the middle of the screen, obstructing the chart
the display to switch to displaying the underlyin
Windows or Linux system screen. Again, even
if no damage has taken place – you still don't
have an ECDIS display!

Worst case scenario?
Captain Richard Madden, writing in the *Maritime Executive*, warns that: 'Anecdotal evidence has shown that difficulties in updatin
ECDIS charts and licenses ensued [as a resul
of charging phones or using unauthorised
USB]'. Beyond that, 'it can be certain that thi
is a potential vector for computer viruses or malware,' he says.

What changes could be made?
Capt. Madden suggests: 'Perhaps it's time the
bridge officers or Master address where these
devices might be charged.'

Dr Andy Norris FRIN FNI

– thwarted by

CYBER SECURITY: ONBOARD SECURITY

An awareness programme for seafarers should cover:

- Emails and how to behave in a safe manner;
- Internet usage, including social media, chat forums and cloud-based file storage where data movement is less controlled and monitored;
- Use of own devices;
- Risks related to installing and maintaining software on company hardware;
- Poor software and data security practices where no anti-virus checks or authenticity verifications are performed;
- Safeguarding user information, passwords and digital certificates;
- The physical presence of non-company personnel, for example where third-party technicians are left to work on equipment without supervision;
- Detecting suspicious activity and how to report if a possible cyber incident is in progress;
- The consequences or impact of cyber incidents to the safety and operations of the ship;
- Understanding how to implement preventative maintenance routines such as anti-virus and anti-malware, patching, backups, and incidence-response planning and testing; and
- Procedures for protecting against service providers' removable media before they are connected to the ship's systems.

Author: Aron Frank Sørensen, Chief Marine Technical Officer at the Baltic and International Maritime Council (BIMCO)

1

Attacks happen

Cyber security should concern everybody, even those who are not computer experts. All seafarers can make a difference.

THE NAVIGATOR

Inspiring professionalism in marine navigators

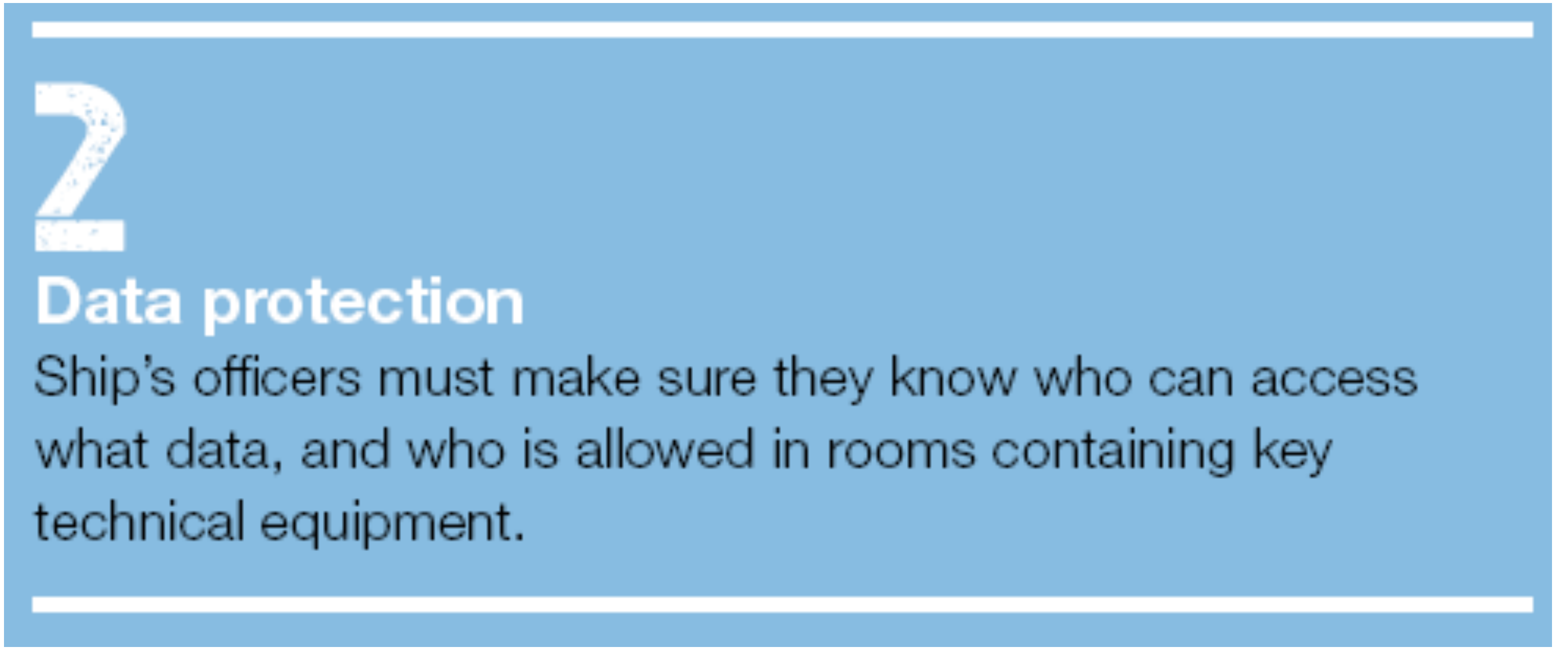
FREE

Cyber Security

Cyber hygiene and the use of ICT on board

The Nautical Institute

A free publication by The Nautical Institute in association with the Royal Institute of Navigation



2

Data protection

Ship's officers must make sure they know who can access what data, and who is allowed in rooms containing key technical equipment.

User Name:
Password:

THE NAVIGATOR
Inspiring professionalism in marine navigators
FREE
Cyber Security
Cyber hygiene and the use of ICT on board
A free publication by The Nautical Institute in association with the Royal Institute of Navigation

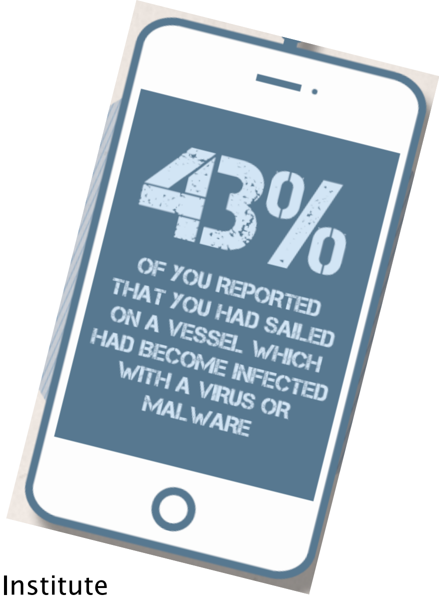
3

Personal risk

Personal devices (smart phones, laptops, USB sticks) and ship systems (navigation, cargo, control, communication) are susceptible to attacks. Connecting personal devices to ship systems for exchanging data or even for charging is highly risky. Don't do it!

IT'S ALL FUN AND GAMES UNTIL YOUR ECDIS FAILS AT A CRITICAL JUNCTURE

THE NAVIGATOR
Inspiring professionalism in marine navigators
FREE
Cyber Security
Cyber hygiene and the use of ICT on board
The Nautical Institute
A free publication by The Nautical Institute in association with the Royal Institute of Navigation

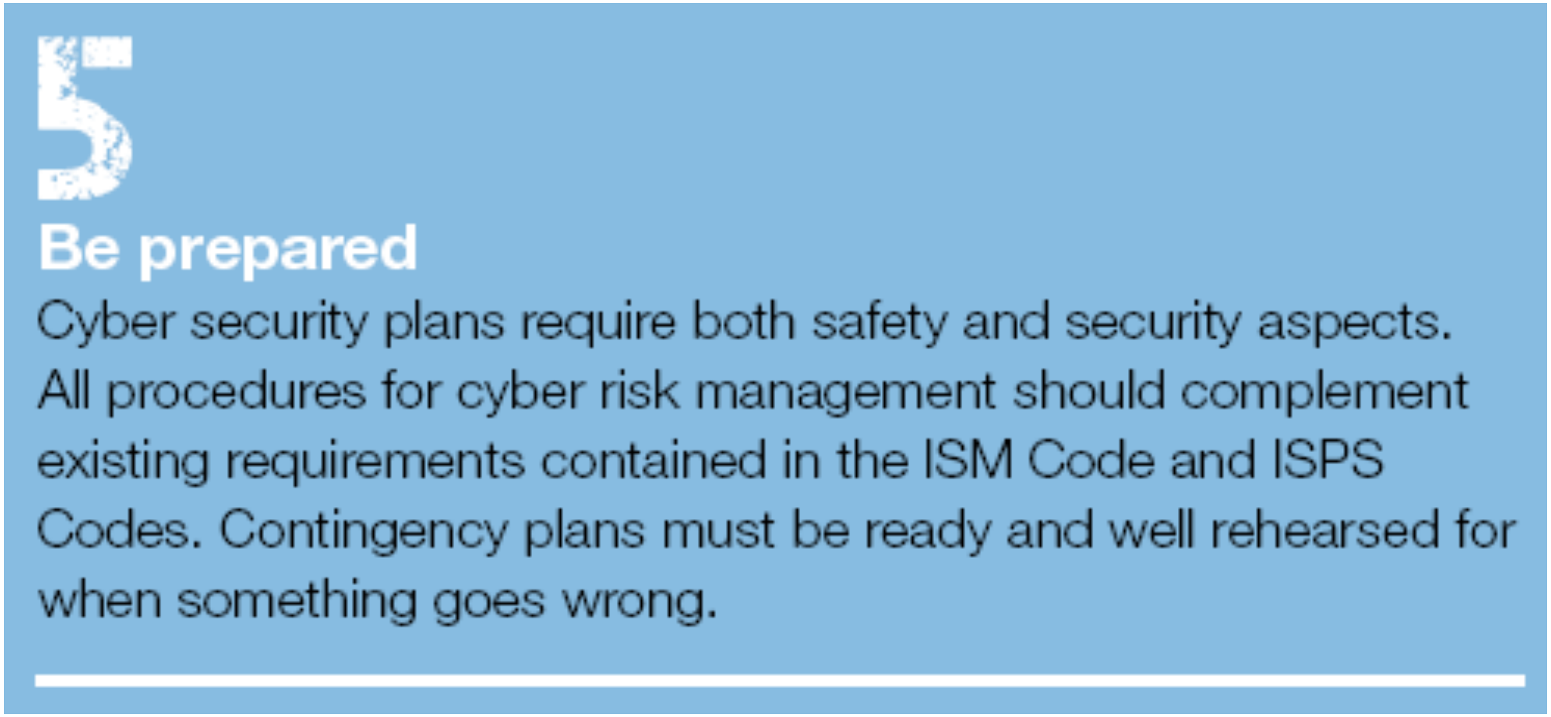

43%
OF YOU REPORTED THAT YOU HAD SAILED ON A VESSEL WHICH HAD BECOME INFECTED WITH A VIRUS OR MALWARE

4

Know your weaknesses

Vulnerable systems include cargo, bridge, propulsion, access control, passenger services, public networks, administrative and crew welfare systems, and all external communication systems.

THE NAVIGATOR
Inspiring professionalism in marine navigators
FREE
Cyber Security
Cyber hygiene and the use of ICT on board
The Nautical Institute
A free publication by The Nautical Institute in association with the Royal Institute of Navigation



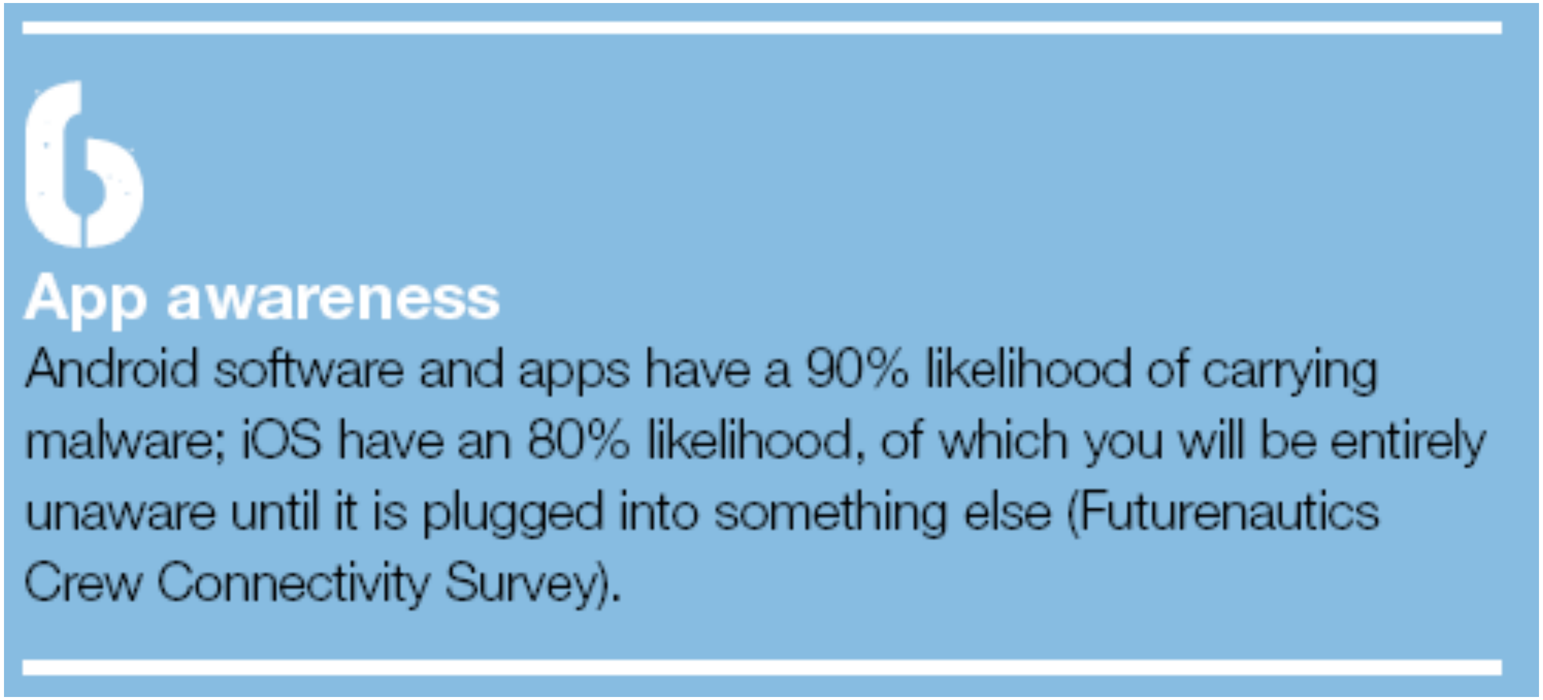
5

Be prepared

Cyber security plans require both safety and security aspects. All procedures for cyber risk management should complement existing requirements contained in the ISM Code and ISPS Codes. Contingency plans must be ready and well rehearsed for when something goes wrong.

ISM CODE
INTERNATIONAL SAFETY MANAGEMENT CODE
AND REVISED GUIDELINES ON IMPLEMENTATION OF THE ISM CODE
2002 EDITION
IMO
INTERNATIONAL MARITIME ORGANIZATION

THE NAVIGATOR
Inspiring professionalism in marine navigators
FREE
Cyber Security
Cyber hygiene and the use of ICT on board
The Nautical Institute
A free publication by The Nautical Institute in association with the Royal Institute of Navigation



6

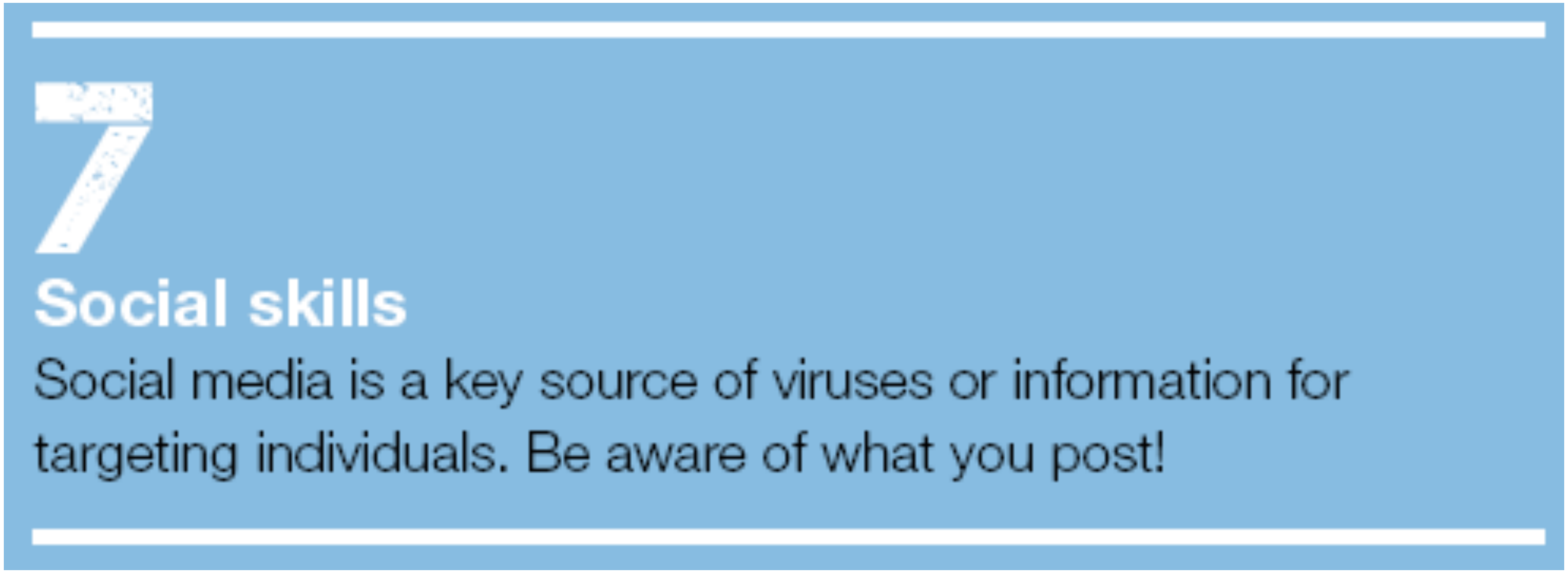
App awareness

Android software and apps have a 90% likelihood of carrying malware; iOS have an 80% likelihood, of which you will be entirely unaware until it is plugged into something else (Futurenautics Crew Connectivity Survey).

“43% of you reported that you had sailed on a vessel which had become infected with a virus or malware. Yet 88% of you claim never to have received any advice or training around cyber security or hygiene”

K.T. Adamson

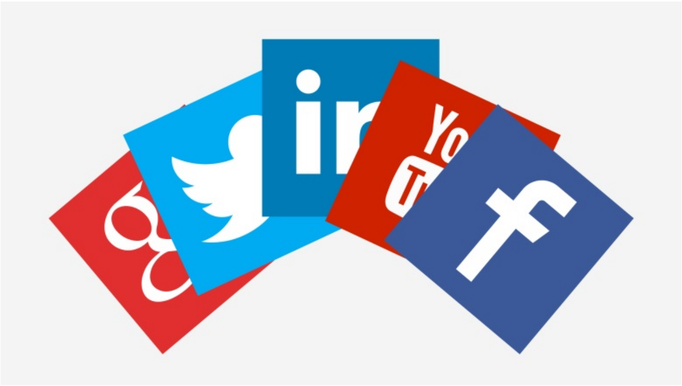
THE NAVIGATOR
Inspiring professionalism in marine navigators
FREE
Cyber Security
Cyber hygiene and the use of ICT on board
The Nautical Institute
A free publication by The Nautical Institute in association with the Royal Institute of Navigation



7

Social skills

Social media is a key source of viruses or information for targeting individuals. Be aware of what you post!

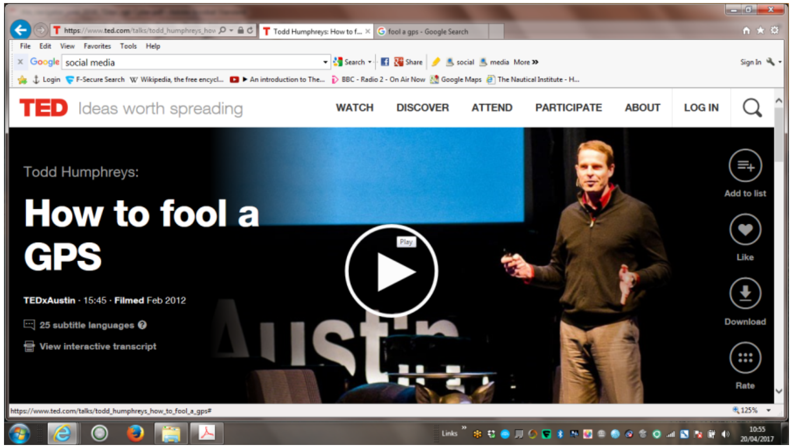


THE NAVIGATOR
Inspiring professionalism in marine navigators
FREE
Cyber Security
Cyber hygiene and the use of ICT on board
The Nautical Institute
A free publication by The Nautical Institute in association with the Royal Institute of Navigation

8

Jamming and spoofing

Global Navigation Satellite Systems (GNSS – including GPS) are vulnerable to intentional and unintentional jamming and spoofing. By following conventional best practice, such as observing radar and visual references, you can minimise the risks.


https://www.ted.com/talks/todd_humphreys_how_to_fool_a_gps

Todd Humphreys:

How to fool a GPS

TEDxAustin · 15:45 · Filmed Feb 2012

25 subtitle languages

View interactive transcript

Todd Humphreys: How to f...
fool a gps - Google Search
File Edit View Favorites Tools Help
Google social media
Search Share social media More
Sign In
Login F-Secure Search Wikipedia, the free encycl... An introduction to The... BBC - Radio 2 - On Air Now Google Maps The Nautical Institute - H...
TED Ideas worth spreading
WATCH
DISCOVER
ATTEND
PARTICIPATE
ABOUT
LOG IN
Add to list
Like
Download
Rate
Play
125%
Links
10:55
20/04/2017

THE NAVIGATOR

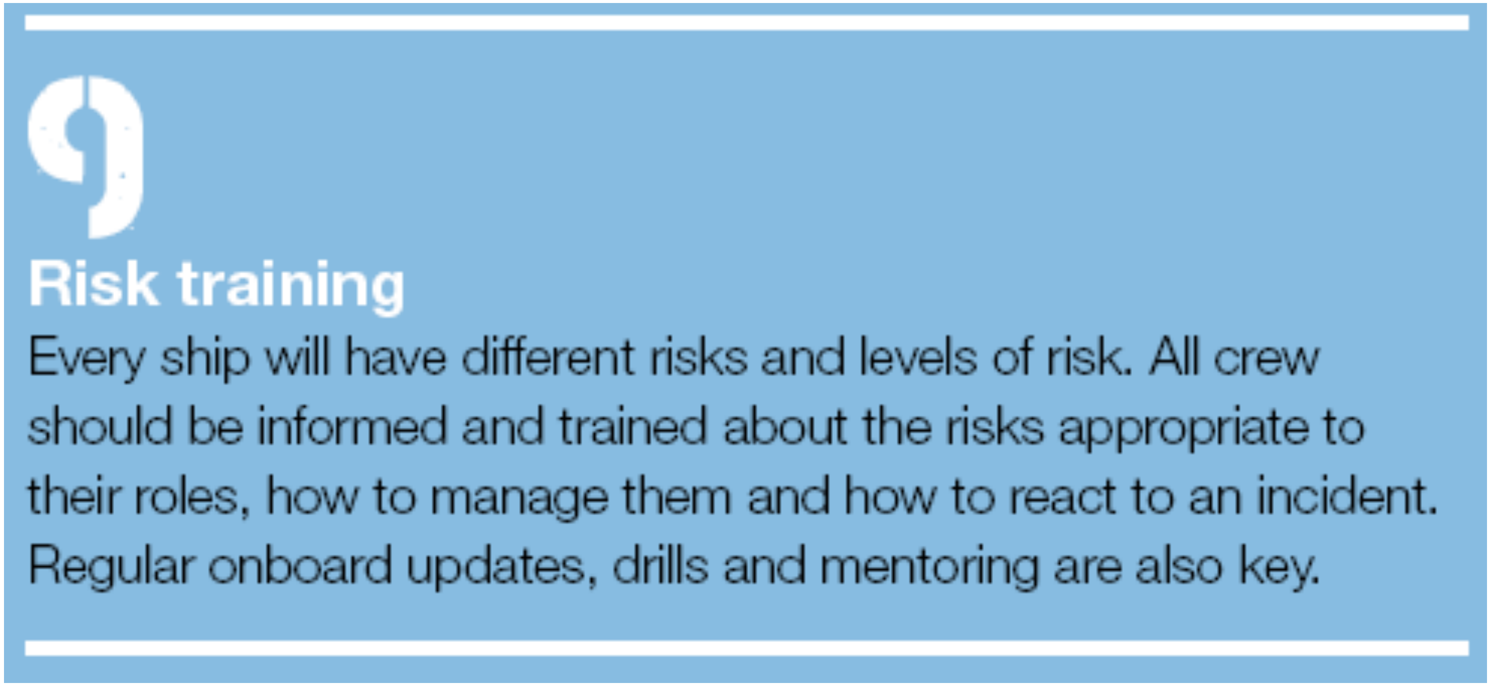
Inspiring professionalism in marine navigators

FREE

Cyber Security

Cyber hygiene and the use of ICT on board

A free publication by The Nautical Institute in association with the Royal Institute of Navigation



9

Risk training

Every ship will have different risks and levels of risk. All crew should be informed and trained about the risks appropriate to their roles, how to manage them and how to react to an incident. Regular onboard updates, drills and mentoring are also key.

THE NAVIGATOR

Inspiring professionalism in marine navigators

FREE

Cyber Security

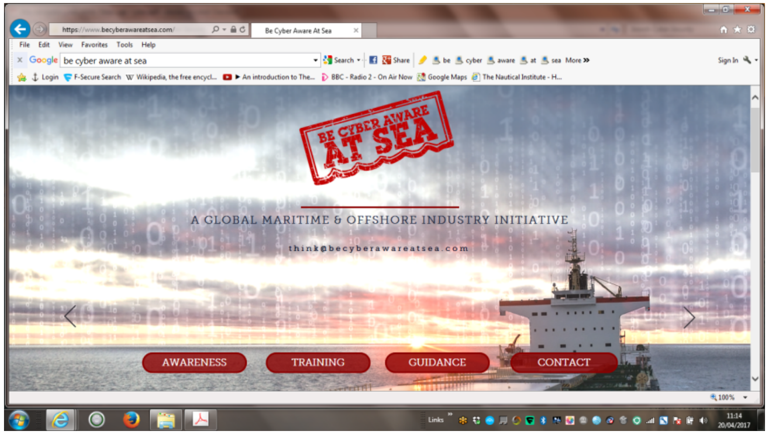
Cyber hygiene and the use of ICT on board

A free publication by The Nautical Institute in association with the Royal Institute of Navigation

10

Want to know more?

Good advice on cyber strategies is widely available online. Specific guidelines for cyber security onboard ships has been published by BIMCO and can be found at www.BIMCO.org


https://www.becyberawareatsea.com/

Be Cyber Aware At Sea

be cyber aware at sea

BE CYBER AWARE AT SEA

A GLOBAL MARITIME & OFFSHORE INDUSTRY INITIATIVE

think@becyberawareatsea.com

THE NAVIGATOR
Inspiring professionalism in marine navigators
FREE
Cyber Security
Cyber hygiene and the use of ICT on board
The Nautical Institute
A free publication by The Nautical Institute in association with the Royal Institute of Navigation

Conclusion

- Risks do exist.
- Risks and mitigation should be identified in SMS.
- Ship & shore staff must be aware.
- Incidents will happen – how will you react?

The Nautical Institute

Support of The Nautical Institute through membership and participation is very much appreciated!

Join Now!

Thank You

The Nautical Institute
202 Lambeth Road, London SE1 7LQ, UK
www.nautinst.org