BEST PRACTICES FOR CYBER SECURITY ON-BOARD SHIPS

Information systems and computer networks have gradually invaded the world of shipping and are now ubiquitous on ships: navigation systems, computers used by the crew, cargo loading management systems, platform management systems (propulsion, electricity, fluids), etc.

This tremendous evolution has involved the emergence of new risks, still underestimated by shipping companies: network intrusion, data theft, remote takeover of computer systems, etc.

Protection against these threats can however be achieved most of the time through simple reflexes. The measures presented in this guide, accessible to non-specialists, contribute to significantly raise the level of computer security on-board ships. The first measures address the crew and, for the most part, should be applied by all its members. The following ones are rather aimed at IT systems managers. This distinction, however, depends on the distribution of roles and responsibilities regarding information systems within the company, between the ship and the headquarters.

Each company is thus invited to make these various recommendations its own and to adapt them to its context and its specific organization.

Thierry COQUIL
Director for Maritime Affairs

Guillaume POUPARD
Director-General of Agence Nationale de la Sécurité des Systèmes d'Information

In a nutshell :

KEY TIPS TO REMEMBER FOR ALL THE CREW

Choose strong passwords

A secure password has at least 8 different types of characters, is not related to the user and is not in the dictionary. Use different passwords on different systems. Do not save your passwords in a file or in an Internet browser, especially when using a public or shared computer.

Use e-mail carefully

Check the identity of the sender. Do not open attachments and do not click on Internet links coming from suspect or unknown senders.

Separate personal and professional uses

Do not transfer your professional email messages to personal messaging. Do not use personal storage devices (USB key, external hard drive, cloud…) to store your business data.

Be careful on the Internet

Social networks, forums, forms, etc. : beware the dissemination of your personal information via the Internet. Before an online payment, check the authenticity and the security level of the website.

Save your data on a regular basis

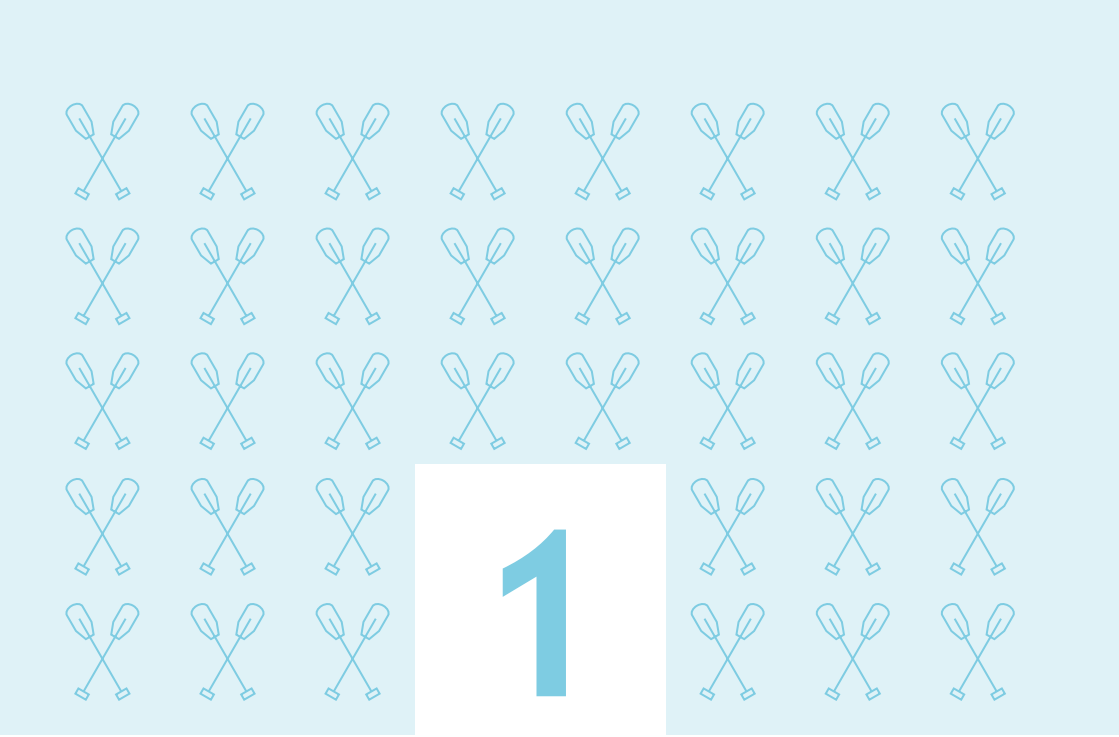
Prepare for a breakdown or a data theft by backing up your data regularly, using dedicated external media, kept safe.

Control installed software on your IT devices

Install only the software you actually need, and always with the prior approval of company administrator. Download your software only from trusted websites and perform regular updates.

I

RECOMMENDATIONS TO CREW MEMBERS



1

Carefully choose passwords

The password is the most frequently used mean to authenticate oneself on digital equipment and thereby access data or control actions. Password quality is essential for proper protection of information and on-board equipment.

A strong password is a password that is difficult to guess with specialized tools but easy to remember. It should have at least 8 characters (ideally 12 characters) of different types (uppercase, lowercase, numbers, special characters).

Choose passwords that are not related to you (name, birthdate, etc.) and that cannot be found in the dictionary [1].

Use different passwords to authenticate on separate systems. Especially, passwords protecting private use (personal messaging, merchant website…) should never be reused in a professional context.

When an account is shared by multiple users, the password must be renewed at each departure or reassignment of a user.

Do not store your passwords in files. If you want to save your passwords, use a dedicated secure solution.

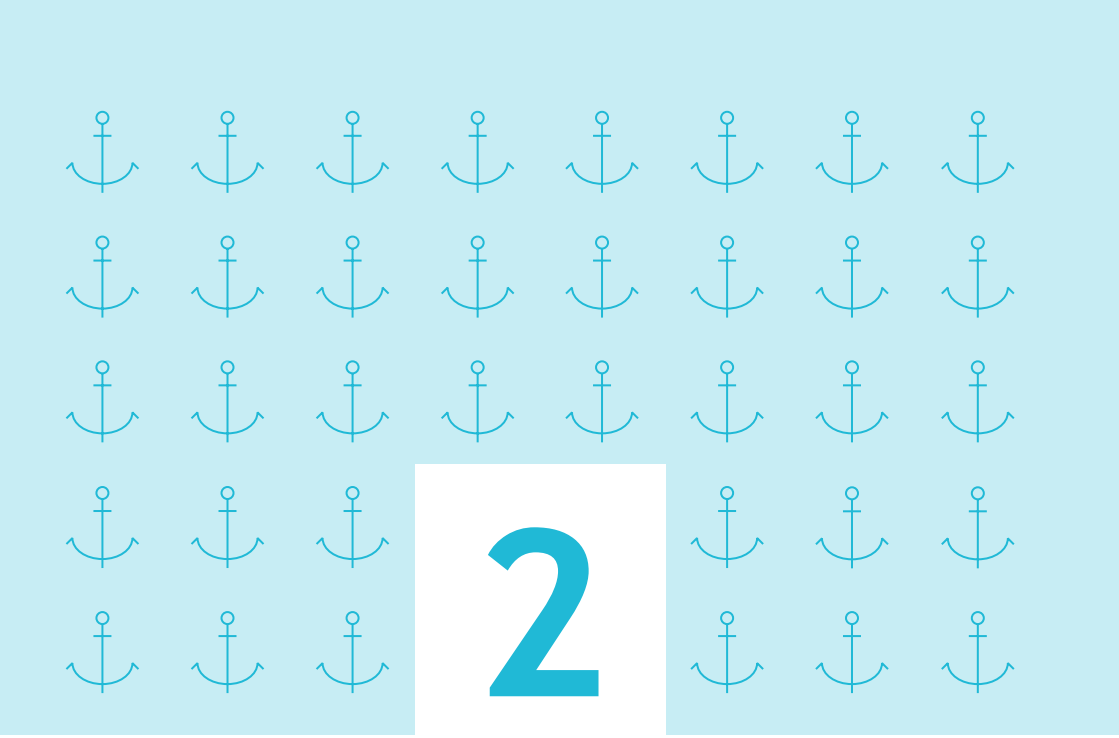
On board :

- define password rules (length, complexity) and ensure they are respected ;
- systematically change default passwords, as soon as possible ;
- do not store passwords in files or on post-it notes ;
- when browsing the Internet, do not store your passwords in browsers, especially when using a public or shared computer.

Beyond the use of a strong password, always lock your session, even during a short absence, to prevent unauthorized access to your workstation.

---

1 : The method of the first letters can help you simply set strong passwords from the lyrics of a song, a proverb, etc. "Where there is a sea, there are pirates!" allows for example to set and remember the password "Wtias,tap!"



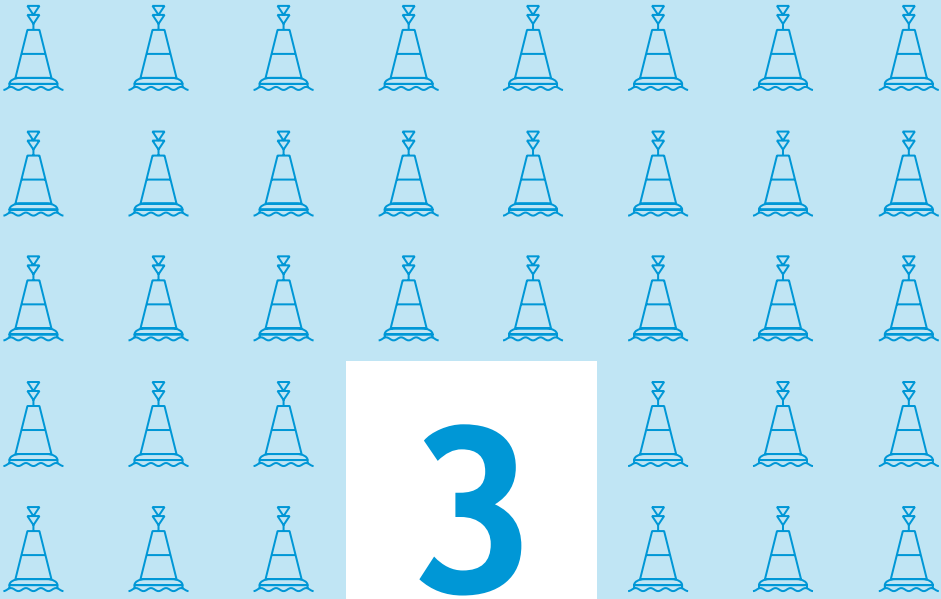
2

Be cautious when using email

Emails and attachments play a key role in the most common computer attacks (fraudulent emails, trapped attachments, etc.). Opening malicious emails may damage the user's computer and jeopardize the entire information system. Thus, all computers on board might be affected.

When you receive emails, take the following precautions :

- the sender's identity is by no means guaranteed, so you must check the consistency between the alleged sender and the message content and check his identity. If there is any doubt, do not hesitate to directly contact the sender ;
- do not open attachments from unknown senders or with unusual title or format ;
- never reply by email to a request about personal or confidential information (ex: PIN code, credit card number). Indeed, some emails ("phishing") imitate the look and feel of well-known institutions in order to steal your data ;
- do not open and do not forward calls for solidarity, virus alerts, etc. ;
- disable automatic opening of downloaded documents.



3

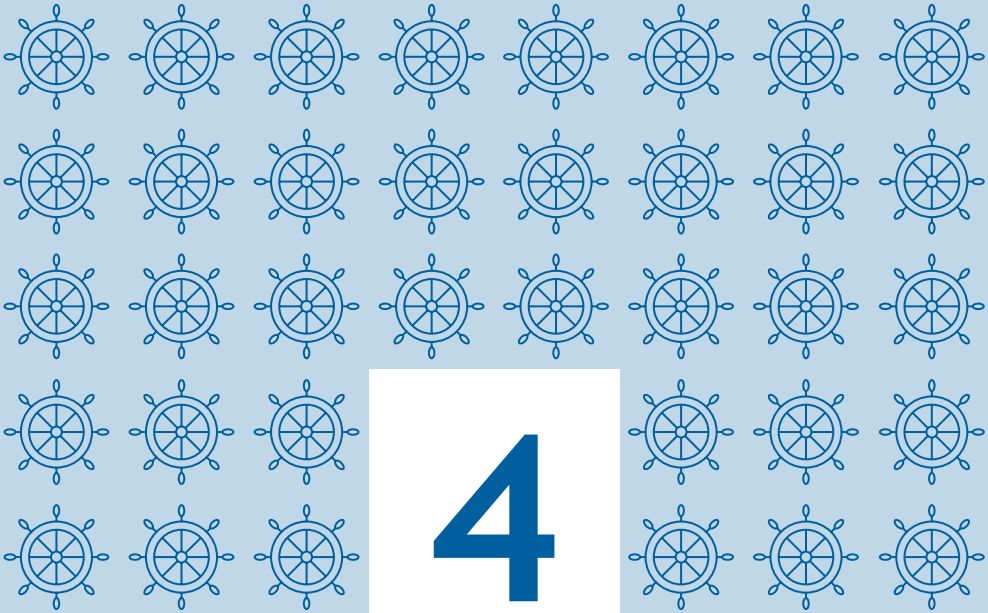
Separate personal and professional uses

Uses and security measures are different on personal and professional devices (laptops, smartphones, etc.).

The use of personal devices in a professional context can affect the safety of ship or company data (theft or loss of devices, intrusion, lack of control over the way devices are used, data leakage in case of departure of a crew member, etc.).

It is therefore recommended to separate personal and professional uses :

- do not forward professional e-mails to personal mailboxes ;
- do not store professional data on personal devices (USB drive, smartphone, etc.) or on personal online storage tools ;
- do not connect personal removable media (USB key, external hard drives, etc.) to the ship's or the company's computers.



4

Be careful on the Internet

Take care of your digital identity and your personal and professional information.

The information you leave on the Internet is no longer under your control. Malicious people can harvest your personal information without your knowledge in order, for instance, to guess your passwords, trap you with personalized emails, access your computer system, etc.

Limit the dissemination of your personal information on the Internet :

- be cautious when requested to fill in forms; transmit only strictly necessary information and remember to uncheck the boxes that would allow the website to store or share your data ;
- reduce to a minimum professional information on social networks, and be cautious about interactions with other users ;
- regularly check your security and privacy settings ;
- use multiple email addresses dedicated to your various Internet activities.

Be careful when paying on the Internet.

When purchasing online, your bank details are likely to be intercepted by hackers directly from your computer. Therefore, before making an online payment, it is necessary to check several elements on the website :

- check the presence of a padlock in the address bar (note: this lock is not visible on all browsers) ;
- make sure the address starts with «https://» ;
- check that the address is correctly spelled.

As a general rule, **never** transmit the 4 digits PIN code of your credit card and do not hesitate to contact your bank to learn about secure payment options.

5

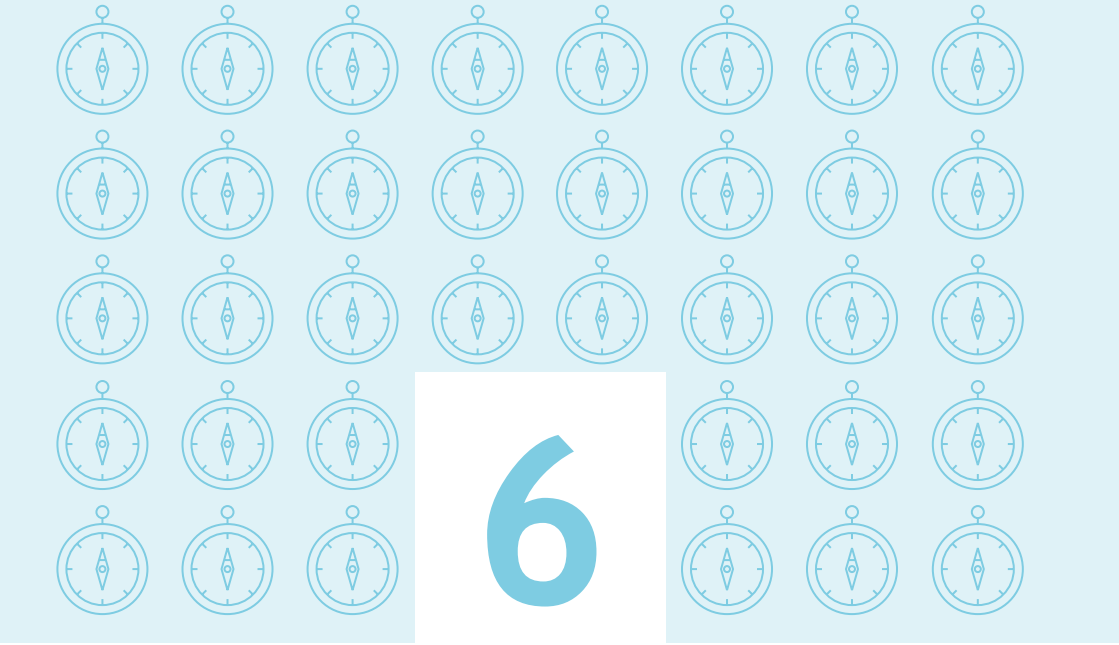
Download your software from the publishers' official websites

If you download content from websites that are not trusted, you take the risk to install malware on your computer. This can allow hackers to take remote control of your computer and, potentially, of onboard IT systems, in order to spy, to steal your personal or professional data, or to launch attacks.

In this context, in order to ensure the security of your computer, your data and the ship :

- do not download your software from sites with doubtful content. Favour reliable publisher websites ;
- remember to uncheck all appropriate boxes to disable the installation of additional software ;
- beware of sponsored links ;
- disable automatic opening of downloaded files.

More generally, never install software or application without the consent of your company's IT advisor.



6

Some additional tips

Be as careful with your smartphone or tablet as with your computer.

While offering innovative services, smartphones are far from being secure. It is therefore essential to follow some basic rules :

- install only necessary applications and check which data they can access before downloading them (location, contacts, phone calls …). Avoid installing applications which require access to data that are not necessary for their operation ;
- in addition to the PIN code protecting your SIM card, use a password to secure access to your device and configure it to lock automatically ;
- make regular backups of your data on an external medium in case your device needs to be restored to its original state ;
- do not store your passwords on your device.

Protect your electronic devices during your travels.

During your trips on shore, be careful if carrying electronic devices (laptop, smartphone, etc.). Travelling with professional mobile devices endangers the information they contain. Thus, you should :

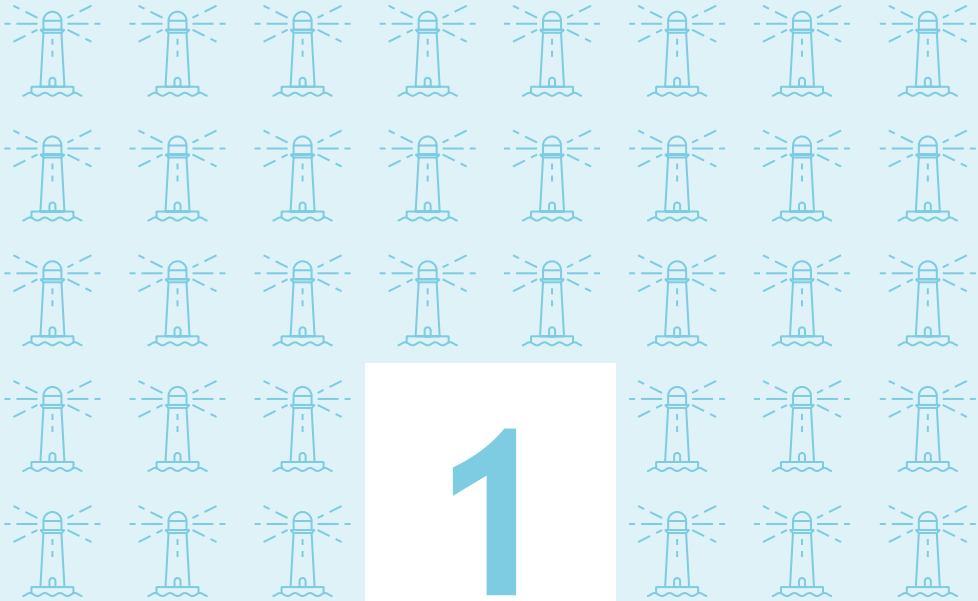
- back up your data, in order to recover them in case of loss or theft of your device ;
- ensure your passwords are not stored in your device ;
- keep your devices and storage media with you (do not leave them in an office and, if they contain sensitive information, do not use the hotel safe) ;
- disable Wi-Fi and Bluetooth when you are not using your devices ;
- if you are forced to leave your phone, turn it off and, if possible, remove the SIM card and the battery ;
- inform your hierarchy in case of inspection or seizure of your device by foreign authorities ;
- never connect your device to an equipment that is not trusted ;
- refuse any connection of an equipment you do not trust to your own devices ;

- never use USB keys offered to you as a gift: corrupted USB keys are commonly used by hackers to infect electronic devices with malware.

Finally, to complement these recommendations, read the information security policy of your company.

II

RECOMMENDATIONS FOR SHIPPING COMPANIES



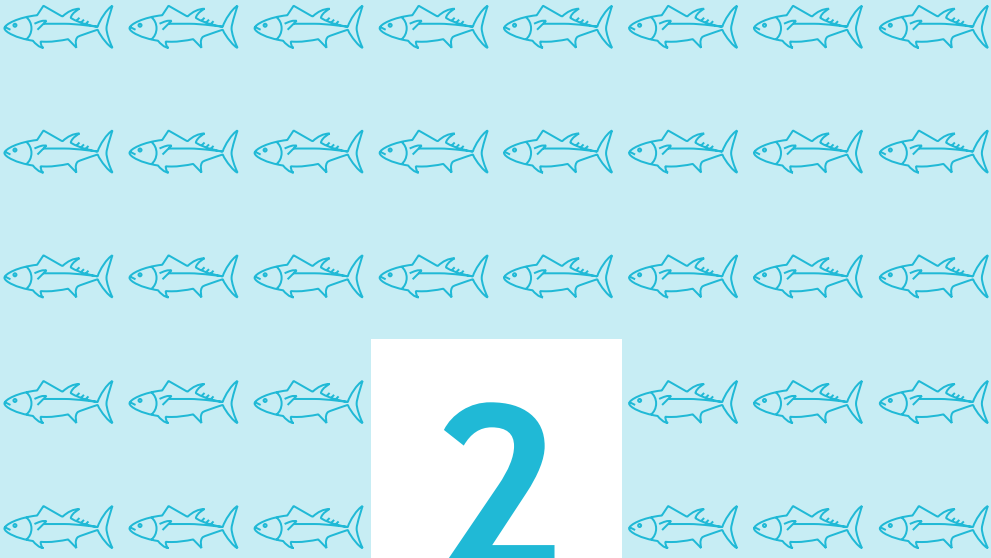
1

Raise staff awareness

The crew's and staff's awareness of IT security good practices is fundamental to effectively reduce the risks related to dangerous behaviour.

Prevention of information system attacks can mostly be achieved through simple reflexes, such as those presented in these guidelines. It is therefore essential that everyone is kept involved and aware, by means of briefings, guidelines and ideally a user charter.

A staff contact for any issues related to IT security must be appointed and clearly identified, particularly on board.



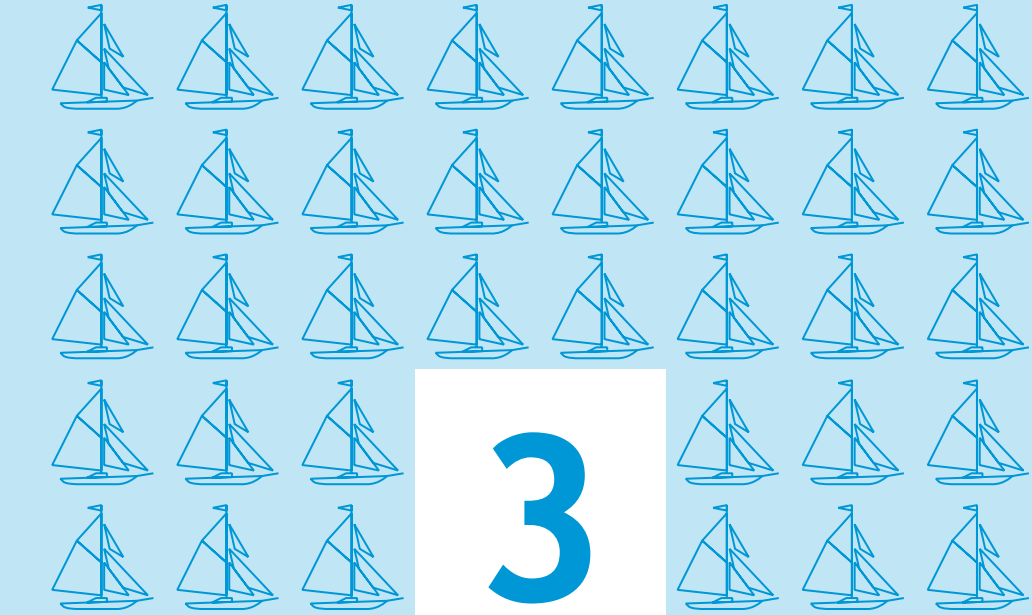
2

Schedule regular backups of your data

To ensure data security on board, it is highly recommended to make regular backups (daily or weekly). You will thus be able to easily recover your data in case of malfunction, error or cyberattack.

External media such as dedicated external drives, recordable CD or DVD, should be available to the crew for data backup. Such media must be stored in a location remote from the backed up system. Attention should be paid to the life duration of such media.

Ideally, a secure storage server network - or NAS (Network Attached Storage) - could be set up on the shipboard network. Such a server is made of several backup disks and thus ensures a high data availability. Spare disks should be available, in case of failure. NAS inspection should be regularly performed to detect potential disk malfunctions as early as possible.



3

Know your users and service providers

Accounts with specific rights are used to log on IT systems. «User» accounts and «Administrator» accounts must be distinguished.

The various accounts on shipboard systems must be created and managed with the utmost attention :

- Only assign administrators accounts to people who strictly need it, because of their duties on board (e.g. electronics officer in charge of IT) ;
- Administrator accounts should be used only for specific operations on the IT system, such as managing user accounts, installing or updating software, maintenance, etc., and should therefore never be used for actions which do not require specific rights (Internet browsing, emailing, etc) ;
- Precisely identify all the users of each IT system and the types of accounts that are assigned to them ;
- Remove any anonymous or generic account ;
- Each user must be identified by name so that each action can be attributed to a user ;
- Define procedures to ensure appropriate granting and removal of user privileges.

4

Regularly update your software

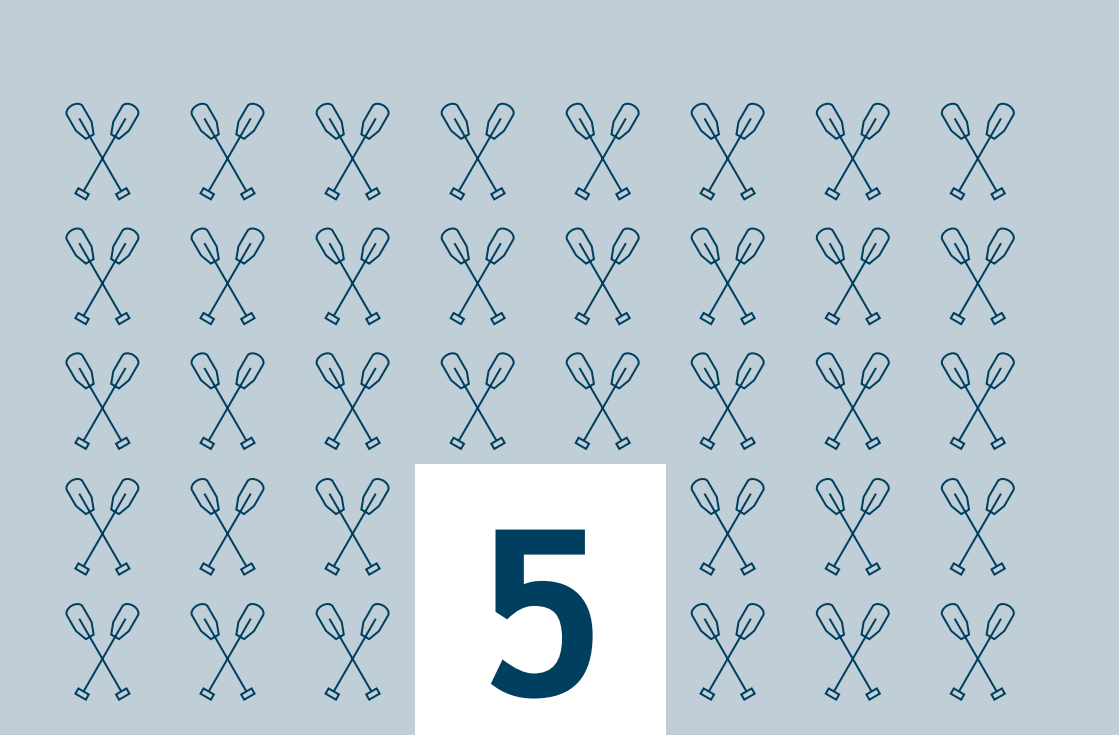
In each software, application or operating system, there are potential vulnerabilities. Once discovered, they are corrected by publishers through security updates. Unfortunately, many users do not perform these updates and hackers can then exploit these vulnerabilities long after their discovery and correction.

It is therefore necessary to define and enforce, for on-board systems, a policy of regular updates, consistent with the constraints of the board.

This policy specifies what has to be updated, who is in charge of these updates, as well as the means to obtain these updates.

Only trusted sources should be used for obtaining updates, such as official websites of publishers.

Functional systems which are essential to the operation of the vessel may be updated on dry dock.



5

Secure on-board Wi-Fi access

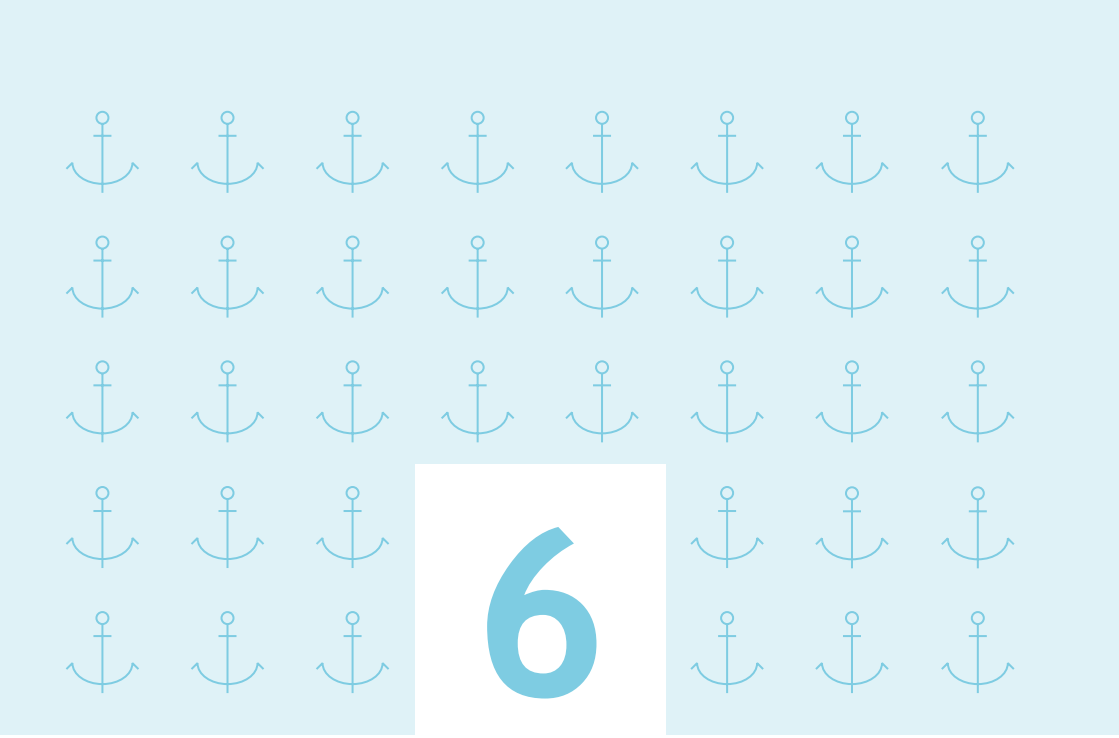
Though the use of Wi-Fi brings agility, an improperly secured Wi-Fi network may allow unauthorized persons to intercept your data and use the Wi-Fi connection without your knowledge to perform malicious operations. When docking, the range of the Wi-Fi signal (a hundred meters) can allow illicit connections to the ship's network from the ground.

Wi-Fi networks must be configured to offer WPA2 encryption protocol. Failing that, WPA-AES should be used (never activate WEP, breakable within a few minutes).

The connection key must be a password of more than 12 characters (using various types of characters). It must only be shared with trusted people and must be regularly changed.

The Wi-Fi network of the ship should allow access only to the network dedicated to the use of personal computers of the crew (sometimes called «Welfare» network).

During stopovers, do not use public Wi-Fi offered in ports, hotels, etc.



6

Partition the network

In a "flat" network, that is to say with no filtering equipment, each device has the ability to access any other. Thus, the damage caused on a single device can easily spread to the entire network. It is particularly important to separate the office network connected to the Internet - which is by nature more exposed to computer attacks - and functional and/or vital systems.

Vital workstations or servers, navigation and control systems of the ship, etc., must be isolated physically or logically from other systems.

It is also recommended to separate professional and private devices into two distinct networks.

Most customer premises equipment offered by Internet satellite providers allow the configuration of two strictly separate virtual networks («VLAN» - virtual local area network). One should be exclusively dedicated to professional IT systems and the other (sometimes called «Welfare VLAN») should be dedicated to personal uses and equipment.

Glossary

- **Antivirus** : software designed to identify, neutralize and delete malicious program.
- **Malware :** malicious program which performs illegitimate and hostile tasks without the user's knowledge.
- **Encryption :** process of encoding a document in such a way that it can only be read by parties in possession of the decryption key.
- **Administrator account :** account allowing modifying network or system parameters.
- **Update :** action of upgrading software by downloading and installing its latest version.
- **Phishing :** hacking technique which consists in sending e-mails imitating the look-and-feel of an institution or a company (bank, tax office…) to induce recipients to provide personal or sensitive information.
- **OS (operating system) :** software which pilots hardware devices and receives instructions from users or other software.
- **Wi-Fi :** wireless network connection.

Version 1.0 — Octobre 2016
20161010-1200

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI — 51, boulevard de la Tour-Maubourg — 75 700 PARIS 07 SP
www.ssi.gouv.fr/communication@ssi.gouv.fr