Loss Prevention Circular KISHPNI-LP-OCT-2022
(What to do about Being Hacked & Safe Browsing)

It comes as no surprise that hackers do not make their victims aware of the fact that they have been hacked. What hackers do is that they penetrate our systems and infect them with a malware in order to take full control. However, there are some important signs that tell us that we might have been hacked.

The malware can remain hidden in the systems without us noticing, while the hacker can access our systems at any time in order to check if the malware planted was able to harass our devices. This is why we might not realize that a hacker is inside our system until it is already too late.

In maritime industry, cyber-attacks on the operational technology (OT) systems have increased with the number of reported incidents set to reach record volumes by year-end.

This happens because where OT networks are thought to be protected, they are often inadequate and based on industrial computerized system, operating in a permanent state of disconnection from the network or, alternatively, connected to port systems and the equipment manufacturer's offices overseas via RF radio communication (Wi-Fi) or a cellular network.

This gives the chance to hackers to access cranes, the storage systems, they can penetrate the core operational systems either through cellular connections, Wi-Fi, and USB sticks, and penetrate these systems directly.

How can seafarers know if they have been hacked:

1-Random browser pop-ups:

If you receive constant, frequent, and random pop-ups while browsing different websites that generally do not show them, it is almost certain that you have been hacked. Nowadays, many websites can bypass ad-blocker programs and show pop-ups. These kinds of websites cannot tell if you have been hacked or not. However, if unexpected pop-ups appear while browsing website that you regularly visit, it is a first sign that something is going wrong with your device.

Announcing that our expertise have taken greatest care for indubitability of the material in this document, Providing guidelines & notices, Permitting the usage of the info & data in training, familiarization and any other possible and legitimate loss prevention activities; KishPNI accepts no Liabilities or claims whatsoever arising from or related to the inadequate use or improper interpretation of the delivered knowledge, advising all recipients to Endeavor the essential Due Diligence in carrying out their management & operational activities upon and through which, KishPNI club is providing support & assistance.

2- Auto-redirect to irrelevant websites:

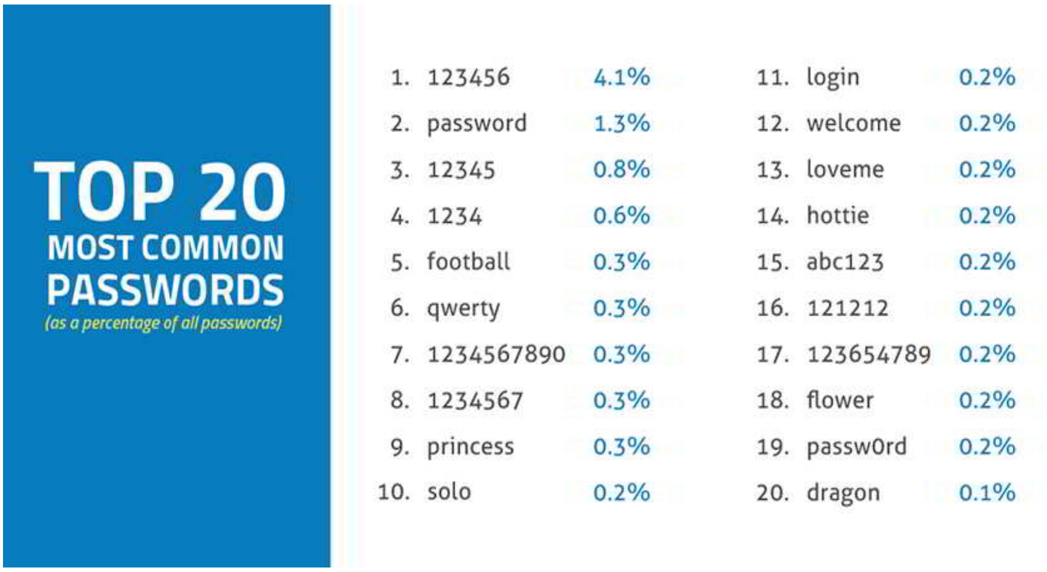
This is one of the most common ways that hackers “inform” you that you have been hacked. Usually, hackers are paid to redirect users to these unwanted websites. Once you open a URL, it will automatically redirect you to a different source without permissions. What happens is that when you enter some keywords in a search bar, the malware installed in your system will automatically redirect you to another website, regardless of what you have been searching before.

3-Messages that you did not send:

We have all witnessed incidents where random messages and links are sent to our inbox from a friend or a person on our contact list. The hacker is using the accounts to send out a message to all our friends with either a link that will instantly start the download of a malicious file or redirect them to a malicious site. This could be a standard message or just a URL. Sometimes, the hackers are personalizing the messages in order to make them appear real and increase the likelihood of someone clicking the link out of curiosity. For example, if a person or a group is telling you to have accessed your account and messaged you about it, you should certainly not click any links that they send, as these are false claims of a further attempt to access personal information. This is a clear sign that our system or social media accounts have been hacked.

4-Unexpectedly wrong passwords:

If you try to log in to a platform or website and the access is denied even though you are 100% sure that you have entered the right credentials, it is crystal clear that your account has been compromised and someone has stolen your details and changed the passwords. What usually happens is that the hacker has previously redirected you to a look-a-like page in order for you to enter your account details, for example to change your password for “security reason”. After that you can be quite sure that the hacker now possesses your credentials and will try to take advantage of your account.



TOP 20 MOST COMMON PASSWORDS

(as a percentage of all passwords)

1.	123456	4.1%	11.	login	0.2%
2.	password	1.3%	12.	welcome	0.2%
3.	12345	0.8%	13.	loveme	0.2%
4.	1234	0.6%	14.	hottie	0.2%
5.	football	0.3%	15.	abc123	0.2%
6.	qwerty	0.3%	16.	121212	0.2%
7.	1234567890	0.3%	17.	123654789	0.2%
8.	1234567	0.3%	18.	flower	0.2%
9.	princess	0.3%	19.	passw0rd	0.2%
10.	solo	0.2%	20.	dragon	0.1%

Announcing that our expertise have taken greatest care for indubitability of the material in this document, Providing guidelines & notices, Permitting the usage of the info & data in training, familiarization and any other possible and legitimate loss prevention activities; KishPNI accepts no Liabilities or claims whatsoever arising from or related to the inadequate use or improper interpretation of the delivered knowledge, advising all recipients to Endeavor the essential Due Diligence in carrying out their management & operational activities upon and through which, KishPNI club is providing support & assistance.

How to protect seafarers from cyber risks:

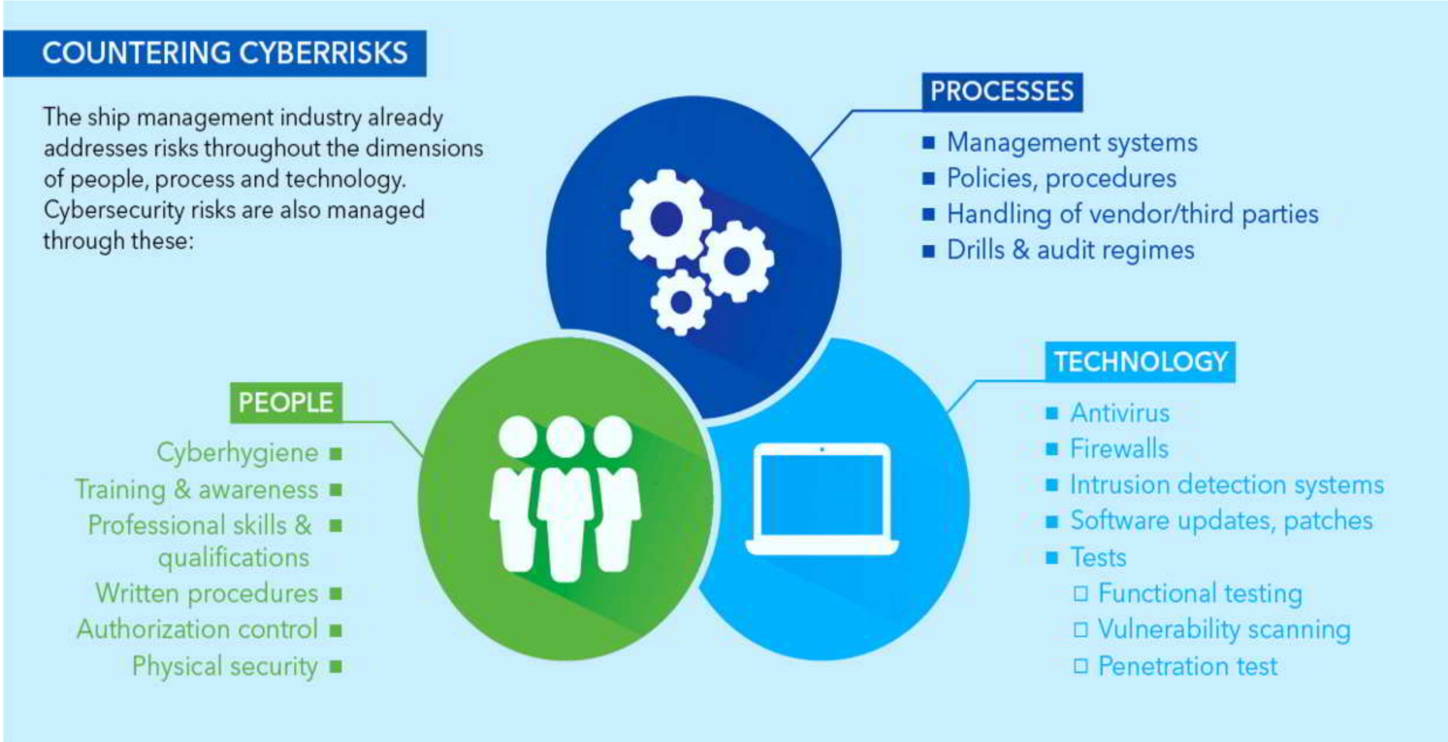
In order to be safe and protect their ships as well from cyber-attacks, seafarers require training regarding internet usage not only on the vessel devices but their private devices as well. Namely, training must take place on software and systems, with seafarers needing to be educated on how to deal with threats from email attacks.

Moreover, crew need to be trained on when to give access, when not to, and how to report these emails if they suspect them to be an attempted hack. In fact, seafarers need to be trained on how to deal with updates, how to deal with password policies, and how to deal in general with onboard IT technology.

This will give them the tools to understand the threats for ship operations because then they will to know what can happen if they open an email, if they give access to somebody who they maybe do not know.

One way that can happen is for shore personnel to inform the crew via regular feedback after a phishing email campaign has been sent out. This allows the seafarers to understand their mistakes and improve their knowledge on what to look out for in an email. This feedback aims to be a constant reminder of the importance of IT security onboard.

The hope is that once seafarers have received increased training on these issues the amount of successful cyber-attacks experienced by the industry will decrease, and the industry will be able to drastically reduce cyber risk and improve operational business, and processes.



COUNTERING CYBERRISKS

The ship management industry already addresses risks throughout the dimensions of people, process and technology. Cybersecurity risks are also managed through these:

PROCESSES

- Management systems
- Policies, procedures
- Handling of vendor/third parties
- Drills & audit regimes

TECHNOLOGY

- Antivirus
- Firewalls
- Intrusion detection systems
- Software updates, patches
- Tests
  - □ Functional testing
  - □ Vulnerability scanning
  - □ Penetration test

PEOPLE

- Cyberhygiene
- Training & awareness
- Professional skills & qualifications
- Written procedures
- Authorization control
- Physical security

Announcing that our expertise have taken greatest care for indubitability of the material in this document, Providing guidelines & notices, Permitting the usage of the info & data in training, familiarization and any other possible and legitimate loss prevention activities; KishPNI accepts no Liabilities or claims whatsoever arising from or related to the inadequate use or improper interpretation of the delivered knowledge, advising all recipients to Endeavor the essential Due Diligence in carrying out their management & operational activities upon and through which, KishPNI club is providing support & assistance.

KISH P&I CLUB

Seven Points for Safe Browsing:

There is no doubt that internet has made our lives easier. The advancements in technology have changed the way we communicate, and the way we do business. How we run our social and personal lives at the moment has nothing to do with what was happening a few years ago. However, because of that, Internet can also threaten us with spam, identity theft, invasion of privacy and cyber espionage.

This is why online safety is critical for today's inter-connected world. It is high time we focused on the positive facet of the digitalized life and learned how to safely browse the Internet.

It comes as no surprise that countless threats are trying to find new ways of compromising our devices where our personal information is stored. Most people would think that visiting a website is like reading a book, but there is much going on in the background that we are certainly not aware of. The data transferred between our devices and the website that we visit, pass through several other computers. For this reason, we are vulnerable to interception at any given moment.

At the moment, the most common threat is "phishing": the type of information theft using deception. What happens is that we are tricked into thinking that we are using the original and legitimate website, and then we are somehow persuaded or made to give our personal information.

A more widespread threat is malware infection. Websites can harbour all sorts of nasty viruses, Trojans, spyware, and adware. Some even without the site owner's knowledge, as malware writers have become very good at injecting their creations into legitimate web pages.

So, what can you do in order to browse the internet safely?

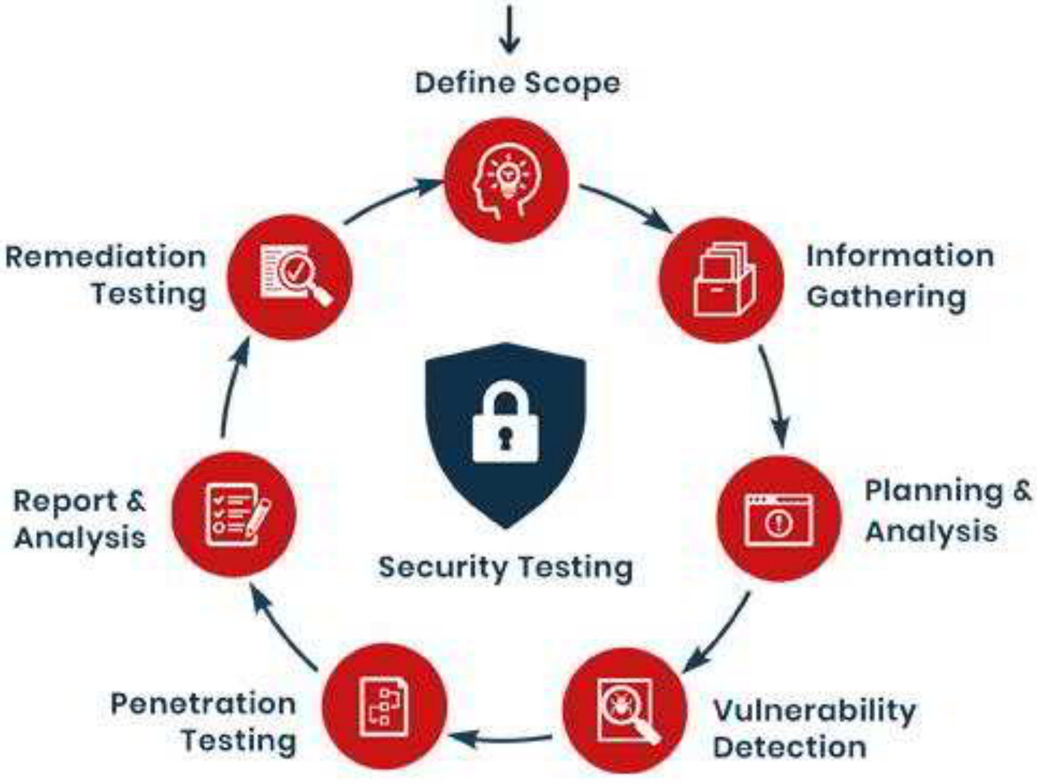
One- Be careful what files you download:

Be careful to not download applications or attachments from "suspicious" websites and sources. Such actions can be the source of virus or malware infection. For this reason, we should download applications only from reputable sources. Also, it is important to scan files for viruses before we click on them. In case we got tricked in downloading an unsafe file, we must cancel the process as soon as possible in the download toolbar.

Announcing that our expertise have taken greatest care for indubitability of the material in this document, Providing guidelines & notices, Permitting the usage of the info & data in training, familiarization and any other possible and legitimate loss prevention activities; KishPNI accepts no Liabilities or claims whatsoever arising from or related to the inadequate use or improper interpretation of the delivered knowledge, advising all recipients to Endeavor the essential Due Diligence in carrying out their management & operational activities upon and through which, KishPNI club is providing support & assistance.

Two-Use the best security software:

Antivirus and firewall protection is critical for maintaining online hygiene. No matter how “careful” we are or how smart we think we are about the links and the files that we click, having a strong and up to date security software is critical. Even in the most “secure” and reputable websites, threats can be well hidden. It is worth investing in a smart antivirus platform that ensures our protection. Today, the most reputable antivirus software solutions use big data and AI in order to monitor running applications and detect/prevent the attacks well before happening.



Three- Consider using an AD blocker:

According to studies, 42% of users globally have installed an ad blocker in their devices. An ad blocker is a tool that uses a number of filters to block specific content, remove distracting ads, block fake news, and thus making it easier to read a website. Except from the user’s convenience, ad blocker also removes the “malvertising” noise and prevents us from downloading dangerous content, since many ads contain malware by “hiding” it.

Four-Use a strong password:

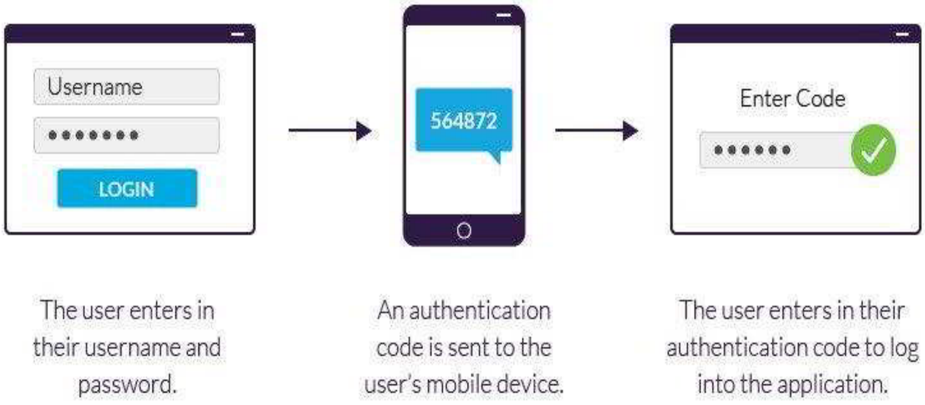
It comes as no surprise that the stronger our password is, the more protected we will be from malicious activities. We should avoid using dates, phone numbers, favorite movies, and sports teams as our password since it is very easy for someone to break or even guess. A strong password should contain special characters, symbols, digits, uppercase letters etc.

Announcing that our expertise have taken greatest care for indubitability of the material in this document, Providing guidelines & notices, Permitting the usage of the info & data in training, familiarization and any other possible and legitimate loss prevention activities; KishPNI accepts no Liabilities or claims whatsoever arising from or related to the inadequate use or improper interpretation of the delivered knowledge, advising all recipients to Endeavor the essential Due Diligence in carrying out their management & operational activities upon and through which, KishPNI club is providing support & assistance.

Five -Enable two-factor authentication (2FA):

It is the simplest, most effective way to verify that your users are who they say they are. Two-factor authentication is a specific type of multi-factor authentication (MFA) that strengthens access security by requiring two methods to verify our identity. These factors can include something only we know – like a username and password – plus something we have – like a smartphone app – to approve authentication requests.

2FA protects against phishing, social engineering and password brute-force attacks and secures your logins from attackers exploiting weak or stolen credentials. Therefore, enabling it will certainly increase the security of our accounts on the internet. Even if somebody guesses our password, they will not be able to access your account.


Username
•••••••
LOGIN
564872
Enter Code
••••••
The user enters in their username and password.
An authentication code is sent to the user's mobile device.
The user enters in their authentication code to log into the application.

Six-Use a Virtual Private Network (VPN):

Most VPN users cite security and privacy reason when choosing this option. VPN is seen as an opportunity to establish a protected network connection when using public networks.

VPN typically works as an intermittent service between us and the host website that we are visiting. It encrypts our data and hides our real IP address. Normally, our information can be viewed by everyone who has network access. However, if our information is encrypted, hackers cannot decrypt our information and thus we are safe.

Seven-Be aware of suspicious URLs:

As a user, it is important to make sure that the websites we are visiting are secure. A quick tip is to pay attention to the left side of the web address. If we see a lock sign, it means that the connection is secure. On the contrary, the exclamation marks tell us that the connection is not secure. The info sign means that the site is not using a private connection.

In addition, we can observe if the website starts with "HTTP" or "HTTPS". The difference between the two is that HTTPS uses Secure Sockets Layer (SSL) in order to encrypt normal HTTP requests and responses. HTTPS is far more secure: if browsers use HTTPS to pass information, it means that the data cannot be read by hackers.

Announcing that our expertise have taken greatest care for indubitability of the material in this document, Providing guidelines & notices, Permitting the usage of the info & data in training, familiarization and any other possible and legitimate loss prevention activities; KishPNI accepts no Liabilities or claims whatsoever arising from or related to the inadequate use or improper interpretation of the delivered knowledge, advising all recipients to Endeavor the essential Due Diligence in carrying out their management & operational activities upon and through which, KishPNI club is providing support & assistance.