#3

FEB:2017

PHISH & SHIPS

BE CYBER AWARE AT SEA

Kindly sponsored by

Novæ

LOOKING FORWARD

BE CYBER AWARE!

Welcome to issue 3 of "Phish & Ships", the maritime cyber security newsletter, keeping you up to date with a new industry initiative, "Be Cyber Aware At Sea".

The campaign has been created to tackle maritime cyber security issues. Providing guidance and raising awareness of cyber threats and risks across the shipping and offshore sectors.

If the threats posed by cyber security weren't enough of a problem, according to a recent article from Reuters - shipping companies are finding insurance policies often fall short.

"Digitalisation" of the shipping industry means that ships are potentially exposed to a range of threats - such as unauthorised interference to electronic navigation devices such as the Global Positioning System (GPS), and attacks on shipboard systems - and as most vessels lack the backup systems, or redundancy these are a major cause for concern. The stakes are high - with people, pollution, vessels and cargo all at risk.

Gaps in insurance for ship owners and the disruptions that could cause, have the potential to drive up both industrial and consumer prices. Reuters bemoaned the fact that information about the nature of attacks is scarce, which insurance and shipping officials say is an obstacle to mitigating the risk. It is hard to set the right cover and to develop products when there is too little actually known.

There is also a gap in provision as most existing cyber or hull insurance policies will not cover the risk of a navigation system being jammed or physical damage to the ship caused by a hacking attack.

There have already been hints at the scale and scope of the potential problems. Just last year, South Korea said hundreds of fishing vessels had returned early to port after its GPS signals were allegedly jammed by North Korea - something the North denies. While an earlier hack by drug traffickers diverted containers in Belgium's Antwerp port.

The warning signs are clearly there, and cyber risks pose a real and present danger to shipping. That is why it is so important to be cyber aware at sea. From seafarers to shipping executives ashore, awareness and training are vital.

RISE OF ONLINE THREATS

According to new data, online fraud is now the most common crime in the UK, with almost one in ten people falling victim, the latest figures have revealed. These figures are likely to be mirrored globally, and all nations will need to manage the threats posed by cyber crime.

The UK figures state that more than five and a half million cyber offences are now thought to take place each year. Incredibly cyber crimes now account for almost half of all offences in the country.

Almost ten per cent of the adult population reports having been a victim of some form of cyber crime. It is the first time that the Office for National Statistics (ONS) has included online offences in the annual survey and the result has seen the overall crime figure almost double.

These figures demonstrate how crime has changed, with fraud now the most commonly experienced offence. This is not a problem restricted to one country - this is a problem on a global scale.

Companies and individuals need to be aware of the threats posed and the ways in which they need to respond. It is also important to report crimes. Unfortunately, just a fraction of offences are currently reported to the police. Victims either feel embarrassed or believe little can be done to catch those responsible. This has to change, and reporting needs to improve.

CYBER SECURITY BASICS

Sharif Gardner, Head of Training at Novae Group shares the basic measures that individuals and organisations should take to reduce exposure:

- **Secure the human.** Educate end users, managers and executive leaders on understanding the most basic of techniques to prevent incidents in the first place. Train your crew to be the human firewall and identify common online threats such as phishing and email scams.
- **Always have up to date anti-virus protection** on IT systems and mobile devices, this will filter most of the known threats.
- **Always update** operating system and application software when instructed to do so by the vendors when possible. They have important security updates and bug fixes. This is not always possible when at sea, so it is important that crew are aware of which systems aren't updated and avoid introducing risks to those systems.
- **Restrict access** to important IT and OT systems and ensure technical and procedural measures to restrict administrator rights. Only those who 'need to know' or be able to change information should be able to do so. This protects the confidentiality, integrity and availability of information.

Sponsored by: Novae LOOKING FORWARD

Gearing Up for New General Data Protection

Are you ready for the new "General Data Protection Regulation" (GDPR) which enters force next year? This is a European regulation intended to strengthen and unify data protection for individuals within the European Union (EU). It also addresses export of personal data outside the EU.

The impact is set to be seismic, and you will need to consider how you deal with it. The way you store and protect data on customers, on seafarers and potentially the way all data is stored will all require attention and reassessment. The regulation applies if the organisation or the data subject (person) is based in the EU. The Regulation also applies to organisations based outside the European Union if they process personal data of EU residents.

The aim of GDPR is to give citizens greater control of their personal data and to simplify the regulatory environment. Compliance is complicated and companies need to ensure they have done enough to meet requirements of all the mandatory Articles of the regulation.
3 key points to be aware of;

- Fines and penalties for a breach have increased to 4% of global turnover or €20 Million, whichever is the HIGHER
- It affects all EU citizens (irrespective of where you operate in the world)
- It affects all businesses irrespective of size

GDPR takes effect on 28th of May 2018, and all companies need to ask tough questions now and should act early to avoid problems.

Cyber Jargon Buster

MALWARE: Software intended to infiltrate and damage or disable computers. Shortened form of malicious software.

PASSING OFF: Making false representation that goods or services are those of another business.

PHISHING: Attempt to obtain sensitive information such as usernames, passwords, and credit card details, by disguising as a trustworthy entity

SCREEN SCRAPER: A virus or physical device that logs information sent to a visual display to capture private or personal information.

WORM: Malware that replicates itself so it can spread to infiltrate other computers.

Driving a Change in Cyber Attitudes...

People and businesses in shipping are sceptical about cyber risks. The issues are often ignored, and usually largely misunderstood – but the threats are real, and need a response.

Thousands of new malicious software and viruses are being discovered along with new software vulnerabilities every single day – so managing a company's exposure to cyber risk has never been more demanding.

As we increasingly turn to hyper-connectivity (machine-to-machine technology communicating with each other) shipping is joining the mix, and as the opportunities to conduct business faster, distribute goods cheaper and operate more efficiently entice – there are risks too.

There is a rush to embrace technology, but with little to no understanding of the security implications related to connectivity. This places seafarers, vessels, systems and operations under increasing risk.

One of the major problems is attitude, rather than technology. Owners and operators seem to feel their ships and cargo are not of interest for 'hackers' –something which is incredibly dangerous. This attitude problems is actually linked to understanding and a lack of awareness.

Maybe hackers can find easier and less risky ways to make money than attacking shipping, but that doesn't mean that shipping companies are immune. They, like any business, have all manner of attractions for criminals. Personal data and financial information, these are the nectar that hacking bees swarm to.

"Be Cyber Aware at Sea" is all about driving change, and opening people to the problems and means of finding solutions. There needs to be a shift in attitude and a response to the threats – not as they are perceived, but as they actually exist.

New Gmail Phishing Fear...

Phishing attacks usually involve bad spelling, obviously fraudulent URLs, or attachments that no one in their right mind would open. But clever cyber criminals know the public is wising up, so they are getting sneakier.

A new Gmail scam is attempting to steal credentials and all starts in a Gmail account that has already been compromised.

Perpetrators access hacked accounts and send phishing messages to other Gmail addresses in the hacked accounts contacts list. An email lands in the target inbox from the hacked address, and here's where it gets tricky: The phishing email uses a legitimate subject line, text, and attachments from emails already sent by that account, making it look completely legitimate.

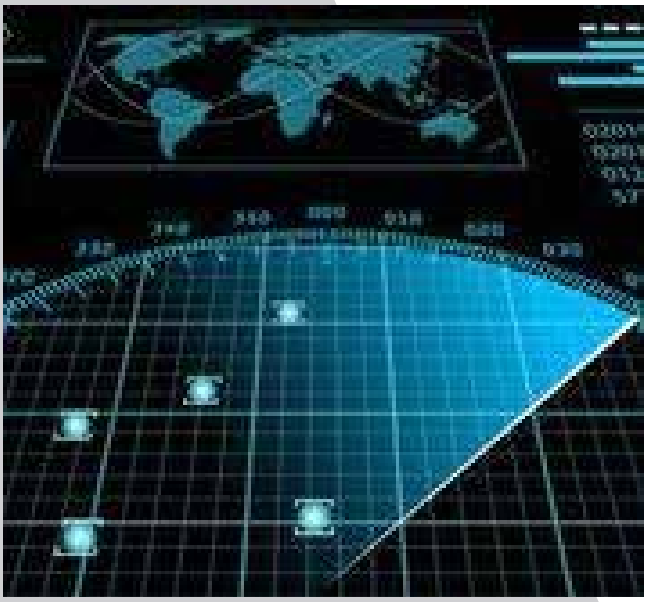
This is one of the trickiest phishing methods yet because it's so hard to detect. So be warned and be careful. Avoiding this attack relies on being wary. When you click on an attachment of any kind be sure to pay attention to the web address in your browser. If it's preceded by data:text/html don't log into it.

Be smart, be cyber aware at sea...

8 Key Steps to Cyber Security Management

1. **Don't do Secure Work on Unsecure Wifi**
2. **Never mix work and personal logins**
3. **Stay away from random USBs**
4. **Don't recycle login credentials**
5. **Don't put off operating system updates**
6. **Always choose two-factor authentication**
7. **Change passwords regularly**
8. **Take cyber security training**

Source: CompTIA



Join in and have your say...

To keep up with the cyber risks to your company, fleet and onboard your ships, make sure you visit our website and join the campaign to make maritime cyber security work.

www.becyberawareatsea.com

think@becyberawareatsea.com

Steven Jones, the editor of this new monthly round-up of maritime cyber matters, would love to hear from you. So please share your thoughts, views and experiences with the industry. We will analyse the current state of play in our next issue.

HYPER CONNECTED SHIPPING: mitigating the cyber threat

TALKING CYBER SENSE: Sharif Gardner, Head of Training at Novae Group shares his thoughts on mitigating cyber threats

Cyber is a threat that should be on every business's risk register, including those in the shipping industry. To date the shipping industry has experienced less attacks than other sectors but this does not mean it is immune or less at risk.

Today's onboard operational technology (OT) and information technology (IT) systems are becoming connected like never before and the reliance on smart and interconnected systems will grow as shipping companies strive to be faster, cheaper and more efficient. This hyper-connectivity greatly increases the risk of critical systems, such as safety, propulsion, or navigation, being exposed to cyber-threats.

Additionally, shipping companies and their vessels are not immune to the relentless threat from cyber-criminals seeking financial rewards, as well as sensitive company or employee information, by using common social engineering techniques such as phishing, business email compromise (BEC), and other basic scams. Whilst certainly not as catastrophic as the loss of a ship's navigation systems, the loss of money and/or critical information can have a significant financial, legal, and reputational impact on the company.

Cyber security awareness across most industries is still relatively poor but according to recent research, it is particularly low in the shipping industry and this needs to change.

Building a strong cyber security awareness culture is the first step. Shipping companies need to recognize and prioritise cyber security in their risk registers and assign accountability for this risk to appropriately qualified senior executives. Contrary to popular opinion, this is NOT an IT issue, it is a business risk and as such it is the executive management team's responsibility to provide all necessary support to effectively develop and promote a culture of awareness.

This is where education becomes important and it is something that needs to happen across every level of the business. Employees are one of the biggest cyber security vulnerabilities and considered a "soft target" by criminals, due to their lack of understanding of the risks faced. Instead of using highly technical and time consuming hacking methods to breach a company's systems, cyber criminals often prefer to target the employees themselves in order to get access to information and systems.

Raising awareness of the cyber threat needs to be a constant process, not a one off box-ticking exercise. We are seeing an alarming rise in business interruption from technology disruptions on board. This is caused largely by untrained crew, or non-malicious insiders as they are known in cyber speak, not recognizing unsafe emails which, when opened download viruses onto the system. Company executives, managers and team leaders need to be regularly communicating the cyber security message, supported by ongoing awareness courses, awareness campaigns, and regular testing.

Heightened awareness will greatly improve a company's ability to effectively manage the cyber security risk, when at sea and onshore. Part of this awareness comes from understanding how the IT and OT systems are connected and where the vulnerabilities lie. Companies need to assess their exposure, explore measures to manage the risk, such as cyber insurance, and develop an incident recovery response plan.

Be Cyber Aware at Sea educational campaigns can help crew in preventing cyber related incidents, however mistakes are inevitable. When this happens, cyber insurance can assist in 'steadying the ship' and keeping an organization operational during uncertain periods of downtime.

Cyber insurance can provide the necessary peace of mind to shipping companies and their vessels. It can cover broad first and third party coverages arising from a computer attack, operational error or accidental damage including cyber extortion and ransomware, customer attrition and transactional e-theft. These insuring agreements offer much wider coverage than traditional P&I policies and are broader than that of just malware and intentional breaches.

Additionally insurers have the advantage of working across a broad range of industries and business types and deal with hundreds of events a year. This allows firms to take advantage of insurer's crisis management vendor relationships to quickly respond to their incident in the most efficient and effective way possible.

With the rate of new malicious software (viruses) and different attack methods increasing every day, and the shipping industry's growing interconnectivity, a cyber-attack is no longer a matter of "if" but "when". The business, financial and reputational impact experienced by a company following an attack will be completely dependent on the measures they implement today to adequately manage the risk. This is a boardroom issue and companies need to act now to educate their employees on the cyber threat, implement a culture of awareness and resilience throughout their organisation and explore other ways to mitigate the risk, such as investing in cyber insurance.

https://www.novae.com/

www.becyberawareatsea.com

think@becyberawareatsea.com

With thanks to our Supporters