CSS PLATINUM

Monthly Security Newsletter.

Season greetings
to you and your families!

The whole CSS Platinum team wish our clients, suppliers and partners a very happy Christmas, and the very best wishes for a prosperous 2023!

How is Maritime addressing Cyber-Security in 2023?

As the maritime industry continues to evolve and rely on a range of technology and digital systems, the need for robust cybersecurity measures has never been greater.

We have seen a vast increase in clients looking to improve the cybersecurity of their vessels. CSS Platinum have provided numerous Security Yacht Audits over 2022 that review vulnerabilities across all digital systems, including navigation, communication, and other critical functions vulnerable to cyber-attacks.

Another priority we are seeing more urgency around is to the security of supply chains. Many maritime companies rely on complex networks of suppliers, partners, and subcontractors, and these can be vulnerable to cyber-attacks. To protect against these attacks, it's crucial for maritime companies to have robust cybersecurity policies and procedures in place and to regularly review and update these policies.

> "CSS Platinum are our cyber task force we use to ensure our clients are cyber resilient and hard to hack. CSS Platinum's mission is to ensure that the cyber risks of building, purchasing, operating and/or chartering a superyacht are understood and that effective mitigation plans are in place prior to our clients taking ownership."
>
> ROBERT ALLEN LAW
> INTEGRATING LAW INTO BUSINESS®

Additionally, the maritime industry needs to focus on improving the cybersecurity of its ports and marinas. These are major hubs of activity, and they are often connected to a wide range of digital systems and networks. As a result, they are attractive targets for cybercriminals. To protect against attacks, these must have robust cybersecurity measures, including firewalls, intrusion detection systems, and regular security updates.

Finally, the maritime industry needs to prioritise the training and education of its workforce when it comes to cybersecurity. Many cyber-attacks are successful because of human error, such as employees clicking on malicious links or sharing sensitive information. To prevent these types of attacks, it's crucial for maritime companies to provide regular cybersecurity training to their employees and to make sure that they understand the risks and how to protect against them. CSS Platinum provide a Cyber Maritime Licence which is the recognised training certification for the Maritime Industry, for more info click here.

In conclusion, the maritime and superyacht industry has many vital priorities regarding cybersecurity. By prioritising these efforts, communities can help ensure that it is prepared to defend against the growing threat of cyber-attacks.

To learn more about how CSS Platinum can help with address cyber-security issue please visit www.cssplatinum.com or contact us directly on support@cssplatinum.com.

CSS PLATINUM

Monthly Security Newsletter.

Keep you & your family safe from cyber-attack over the festive season

As the holiday season approaches, many people are looking forward to spending time with their loved ones, exchanging gifts, and enjoying the festive atmosphere.

However, it's important to remember that the holiday season can also be a prime time for cybercriminals to target unsuspecting individuals and organisations. This article will discuss the vital steps to protect yourself and your loved ones from cyber-attacks during Christmas.

First and foremost, it's essential to be mindful of the types of scams common during the holiday season. One common scam is the "fake business" scam, where criminals create fake websites or social media pages for organisations such as charities. Do your research and verify that the organisation is legitimate.

Another common scam is the "gift card" scam, where criminals send fake emails or messages claiming to be from a retailer and ask the recipient to purchase gift cards for payment. These gift cards are often untraceable, so once the victim has purchased them, the criminal can easily redeem them for cash. To avoid falling victim to this scam, never give out your personal or financial information in response to unsolicited emails or messages, and be cautious when purchasing gift cards.

One of the best ways to protect yourself from cyber-attacks during the festive season is to practice good "cyber hygiene." This means taking basic steps to secure your devices, such as using strong, unique passwords for each of your accounts, and regularly updating your security software. It's also a good idea to use two-factor authentication whenever possible, providing an additional layer of security.

Additionally, be cautious when using public Wi-Fi networks, as these can be vulnerable to attacks. Avoid accessing sensitive information (such as your bank account or credit card information) while using public Wi-Fi, and consider using a virtual private network (VPN) to encrypt your internet traffic and protect your data.

Finally, educating yourself and your loved ones about the potential risks of cyber-attacks is essential. Please encourage your family and friends to be vigilant and cautious when online, and remind them never to give out personal or financial information in response to unsolicited emails or messages.

The holiday season is a time for celebration and joy, but it's also a time to be extra vigilant and resilient about protecting yourself from cyber-attacks.

Always be hard hack!

Be resilient and have a very

from all at CSS Platinum.