CSS PLATINUM

Monthly Security Newsletter.

CSS Platinum Newsletter March Edition

As we head into charter season, we are looking forward to joining the marine and superyacht communities at the 40th anniversary celebrations of the Palm Beach boat show starting today!

We are also celebrating our own team this month as part of International Womens Day, as well as highlighting the on-going security threat posed by phishing attacks making you #hardtohack

40TH PALM BEACH INTERNATIONAL BOAT SHOW

How a Maritime Cyber Licence can help meet IMO ISM Regulations

CSS Platinum provide a range of IMO Compliance services to ensure a vessel and organisation meet the requirements of the IMO International Safety Management (ISM) regulations for Cyber Risk Management.

Our Maritime Cyber Licence recognises and certifies to the latest cyber security guidelines and provides:

- Trained Cyber Aware Team and Crew
- Certification for Safety & Security
- Meet Cyber Risk Management Guidelines
- Secure and Safe Vessel
- Lower Insurance Premiums
- Adhere to Compliance & Security Regulations

CYBER MARITIME LICENSED

IMO CYBER COMPLIANCE

Learn more about Maritime Cyber Licence

Download PDF

Team Spotlight: International Women's Day

CSS Platinum's Director of Information Security, Charlotte Riley was asked to discuss her background and experiences as a woman in business on International Women's Day!

As one of the founders of CSS Platinum Charlotte ensures the business is one that is not only supportive but also diverse and empowering, "driving a level of understanding between people is so important, we create a positive environment, so everyone works more effectively together. It's important for women to be successful in the workplace, but equally there are gender stereotypes and inequalities for men also."

Charlotte Riley began her career in the Army before moving to the US to work at NATO. She is now CTO and a founding member of cyber security specialist CSS Platinum.

CSS PLATINUM

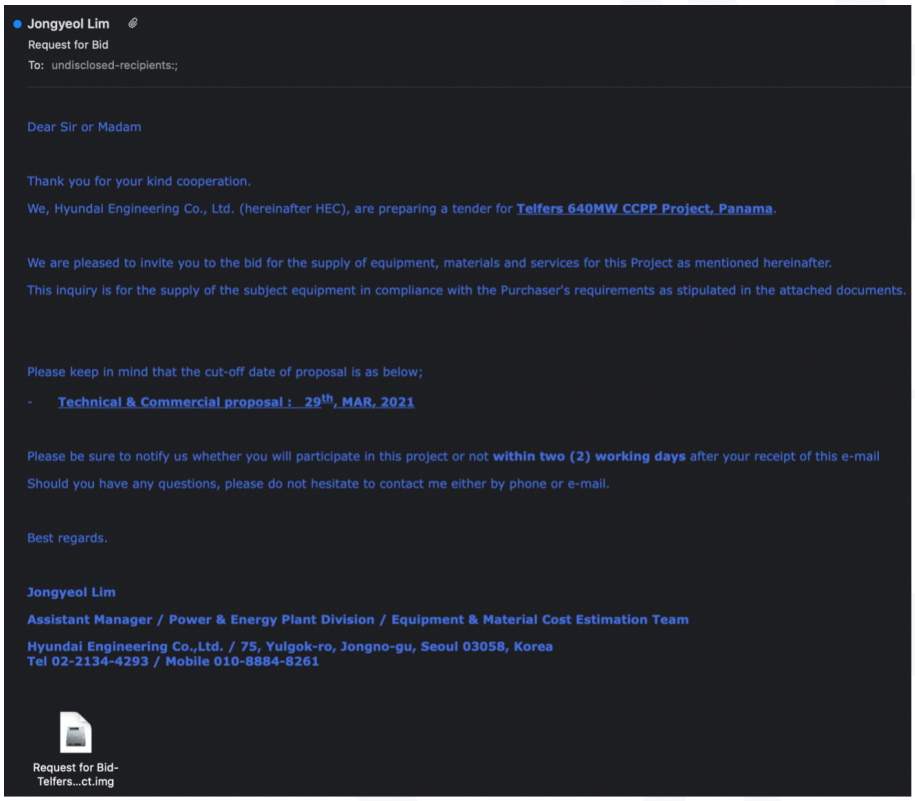
Monthly Security Newsletter.

Attacked: the Phishing hack that has plagued the oil & gas industry

The spear-phishing campaign targeting the Oil & Gas industry was discovered in July 2021 but remains active today, presenting a unique and persistent threat.

This phishing attack delivered a malware file to an internal employee via email, as per the example below. The only action then required to initiate the malware is for an employee to open the file – a double click that can compromise an entire organisation.

The emails are specifically formatted to appear like valid correspondence between two companies tailored to the intended recipient, utilising information obtained on social media regarding the employee and/or the company. Unique requests for quotations (RFQ), contracts, and referrals/tenders to real projects related to the business of the targeted company increases the credibility of the emails and lure victims into opening the malicious attachments.



Jongyeol Lim

Request for Bid

To: undisclosed-recipients:;

Dear Sir or Madam

Thank you for your kind cooperation.

We, Hyundai Engineering Co., Ltd. (hereinafter HEC), are preparing a tender for **Telfers 640MW CCPP Project, Panama**.

We are pleased to invite you to the bid for the supply of equipment, materials and services for this Project as mentioned hereinafter.

This inquiry is for the supply of the subject equipment in compliance with the Purchaser's requirements as stipulated in the attached documents.

Please keep in mind that the cut-off date of proposal is as below;

- **Technical & Commercial proposal : 29th, MAR, 2021**

Please be sure to notify us whether you will participate in this project or not **within two (2) working days** after your receipt of this e-mail

Should you have any questions, please do not hesitate to contact me either by phone or e-mail.

Best regards.

Jongyeol Lim

Assistant Manager / Power & Energy Plant Division / Equipment & Material Cost Estimation Team

Hyundai Engineering Co.,Ltd. / 75, Yulgok-ro, Jongno-gu, Seoul 03058, Korea
Tel 02-2134-4293 / Mobile 010-8884-8261

Request for Bid-Telfers...ct.img

Additionally, consider the reputational risk to your organisation. The phishing campaign not only compromises the security of your network, but it also seeks to use the harvested user credentials to impersonate the victim online to its customers or partners.

Speak to our specialists about how to prevent phishing and cyber-attacks support@cssplatinum.com.