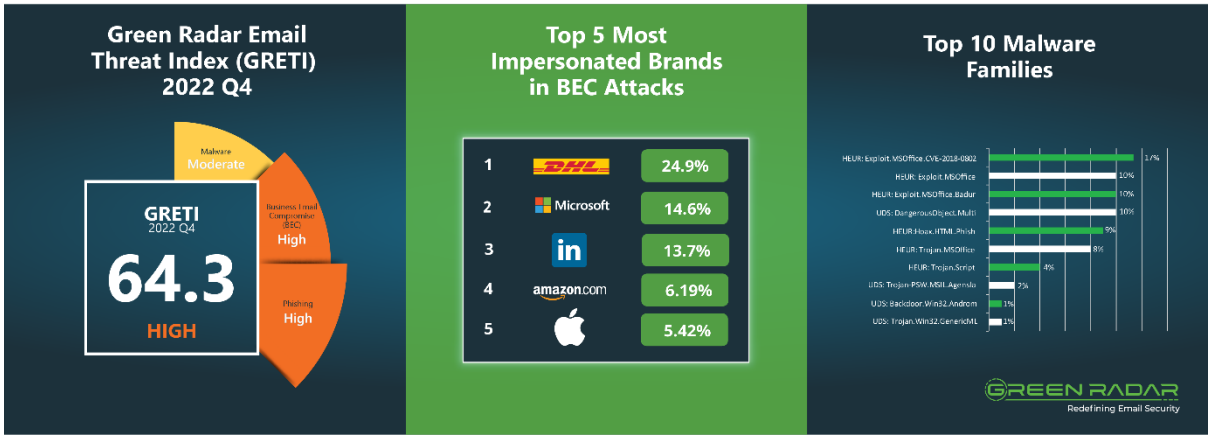
[For Immediate Release]

GREEN RADAR (HONG KONG) LIMITED

Green Radar Announces Email Threat Index for Q4 2022
grMail is recognised by Frost & Sullivan as a email security leader in Hong Kong & Singapore

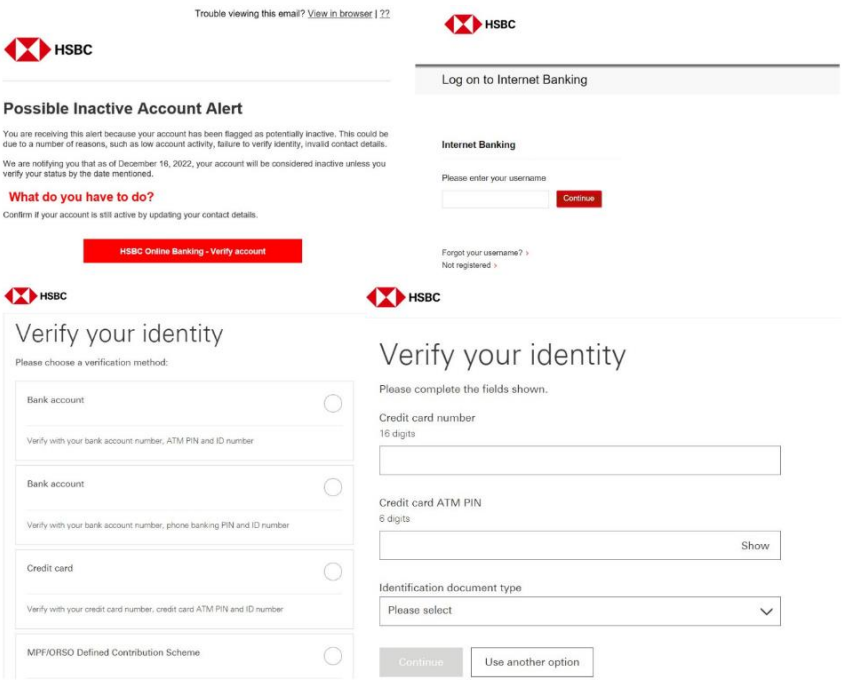
(2nd February 2023, Hong Kong) Green Radar (Hong Kong) Limited ("Green Radar" or "Company") has released the Green Radar Email Threat Index ("GRETI" or "Index") for the fourth quarter of 2022. The index for this quarter is 64.3 (the index released in October was 68.1), suggesting that the risk of email threats has moderately decreased. The overall the risk level remains "High" despite the moderation of phishing and Business Email Compromise (BEC) attacks, due to the continuous evasive and high volume of evasive attacks monitored. This report revealed that hackers sent out mass emails at the end of the year, took advantage of the public's anticipation of annual bonuses and attempted phishing by impersonating companies' financial departments. The FSI("financial service industry") sector continues to be a prime target for phishing attack campaigns. Meanwhile, grMail, the premier product that Green Radar offers to protect organizations against email threats, was recognised by market research company Frost & Sullivan in January 2023 as a leader in email security in Hong Kong and Singapore, reflecting the technological and sophistication of the product in these two operating regions.[1]



DHL reclaims the top spot of the most impersonated brand listing, while Apple debuts its presence with a fifth place

According to the GRETI Q4 report, commercial email scam attacks have decreased compared to the previous quarter. Green Radar Email Security Operations Centre (SOC) statistics showed that the top three most impersonated brands are DHL, Microsoft and LinkedIn. Besides, although HSBC could not reach the top 5, SOC intercepted numerous related phishing emails. Prevalent contents mimicked "Inactive Account Alert", lured users to click the link and "re-activate" the account, hence attempted to steal their personal information and credentials. According to the Green Radar SOC data, more than 1,000 phishing attacks with hyperlinks were triggered daily, implying that corporates are easily exposed to hackers' attacks without ample protection from email security solution providers, leading to unforeseen losses.

[1] The Frost &Sullivan Report, 1 January 23.
https://www.frostchina.com/content/insight/detail?id=63d89cd29c446c956d93bc81



（An example of a phishing email impersonating HSBC provided by Green Radar SOC）

HEUR:Exploit.MSOffice.CVE-2018-0802 rose from the third place to the top among malwares. HEUR: Exploit.MSOffice remained at the second place. HEUR: Exploit.MSOffice.Badur made its way to the top three from the fifth place, showing that such malware is popular among hackers and more attention is needed.

Internal Awareness training is effective against the phishing crisis

It is essential to understand your company's internal threats and provide employees with a proper phishing awareness assessment, hackers are known to target the weakest point in a business, and employees are a potential threat. As mentioned before, there were more than 1,000 phishing attacks daily. Every attack represents a risk of data leakage, ransomware and fraud to enterprises. Inadvertent disclosure of data by employees due to accident or negligence, such as bypassing IT security controls and related security settings while working remotely, would allow hackers to access sensitive and confidential information without authorisation.

Therefore, improving employees' security awareness can equip them as the frontline of defence against cyber attacks. Green Radar's grAssessment (Phishing Awareness Training) can tailor solutions for corporates, increase employees' awareness of email threats and fortify the security barrier. According to the statistics of SOC, it is found that after the second phishing awareness training was conducted, employees' security awareness increased by at least 51%.

Quishing techniques still running rampant, 'issuing' year-end bonuses impersonating finance departments

According to phishing emails provided by Green Radar SOC, hackers were adept at manipulating the public's emotions and leveraging the hot topics in town. By the end of the year, nearly 38% of phishing emails were sent under the guise of the finance departments. Hackers target specific groups and craft persuasive email content for profit.

The email contained a QR Code photo of a phishing website, which lured the recipient to scan and open the link to the fake website. The account would be in the wrong hands if users fall into the trap. QR Code is an image file, which can easily bypass the security systems. Fortunately, there are existing

technologies on the market to deal with this type of attack such as grMail's AI technology, one of the solutions provided by Green Radar, it can precisely identify malicious links, attachments, and QR Codes in emails.


转发：关于财务部 2022 年个人劳动补贴申领通知

《2022 年财政个人劳动补贴》声明

1、根据国家财政部、国家税务总局、国家市场监督管理总局、工商行政管理局联合下发《2022 年财政劳动补贴》现已开展。

2、工资补贴、疫情补贴、社保补贴、医保补贴、毕业生补贴、中高级技工生活补贴、工龄补贴、交通补贴、医疗保险、失业保险、生育保险等。

3、银行账户将会多出一笔补贴，收到通知后，请立即使用手机扫一扫以下二维码认证领取。

该通知上周已经送达各单位，未完成登记的请抓紧登记，本周未完成视为放弃申领！

微信扫一扫，按照提示操作领取

主办单位：国务院办公厅 运行维护单位：中国政府网运行中心

版权所有：中国政府网 中文域名：中国政府网.政务

京 ICP 备 05070218 号 京公网安备 11010202000001 号

(An example of hackers creating phishing emails with a QR code)

Mr. Francis Lee, Executive VP, Product Marketing at Green Radar, commented, "Cybercrime is getting more advanced, and its tactics against businesses are getting more sophisticated. For the company to have an adequate defence to withstand email attacks, besides choosing an excellent email security service provider, cybersecurity awareness exercises for employees are also indispensable." Regarding grMail being acknowledged as the leader of email security service provider, he added, "Frost & Sullivan's report is an important recognition of Green Radar's technology research and development. We are dedicated to providing corporate customers with the most tailored and comprehensive email protection solutions, continuously advancing the technology of grMail to enhance local threat intelligence, detection and interception capabilities."

About Green Radar

Green Radar redefines email security and enables organisations to focus on running their business. We take a Managed Detection & Response (MDR) approach to protect organisations from email threats by combining big data with artificial intelligence, global threat intelligence and a team of cybersecurity experts to keep your inbox safe. Green Radar was recognised by market research company Frost & Sullivan in 2023 as a leader in email security market in Hong Kong and Singapore, leading the field in terms of technological comprehensiveness and innovation.

Green Radar is a member of Edvance International Holdings Limited (1410.HK), a leading cybersecurity and innovative technology company headquartered in Hong Kong.

Company website: https://www.greenradar.com/

For Media enquiries, please contact：

Across Asia Communications Limited
Mr Adrian Wong/ Mr Kent Lau
Tel： +852 6282 6412 / +852 9750 5105
Email: adrian.wong@acrossasia.hk / kent.lau@acrossasia.hk

Green Radar (Hong Kong) Limited
Ms Carol Yip
Tel： +852 3194 2266
Email： carol.yip@greenradar.com

Issued by Green Radar (Hong Kong) Limited