GREEN RADAR

Redefining Email Security

HKCSS x Green Radar NGO Webinar

How to detect and protect organization from phishing attack effectively

網絡釣魚電郵之防範及保安應對工作坊

Date: 20 July 2022 (Wednesday)

July 2022

Table of Content

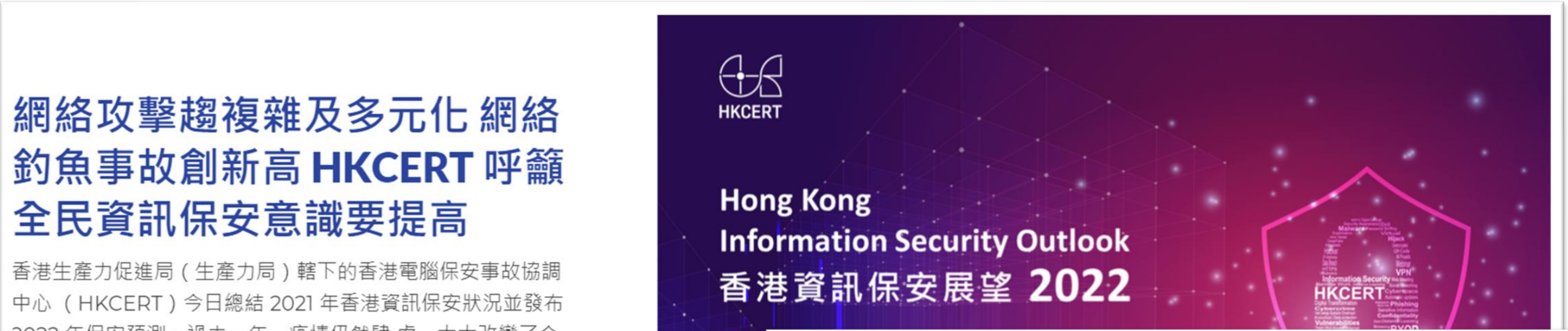
01 **Advice from HKCERT and HK Police**
What is phishing ? How bad is it? Why NGO needs email security protection?

02 **Common Attack Samples**
Phishing attacks commonly seen in HK NGO environment

03 **grMail + grAssessment**
Technology available in the market to protect your organization from phishing attack

04 **Green Radar Company Background**
Who are we? Reference of existing Green Radar customers

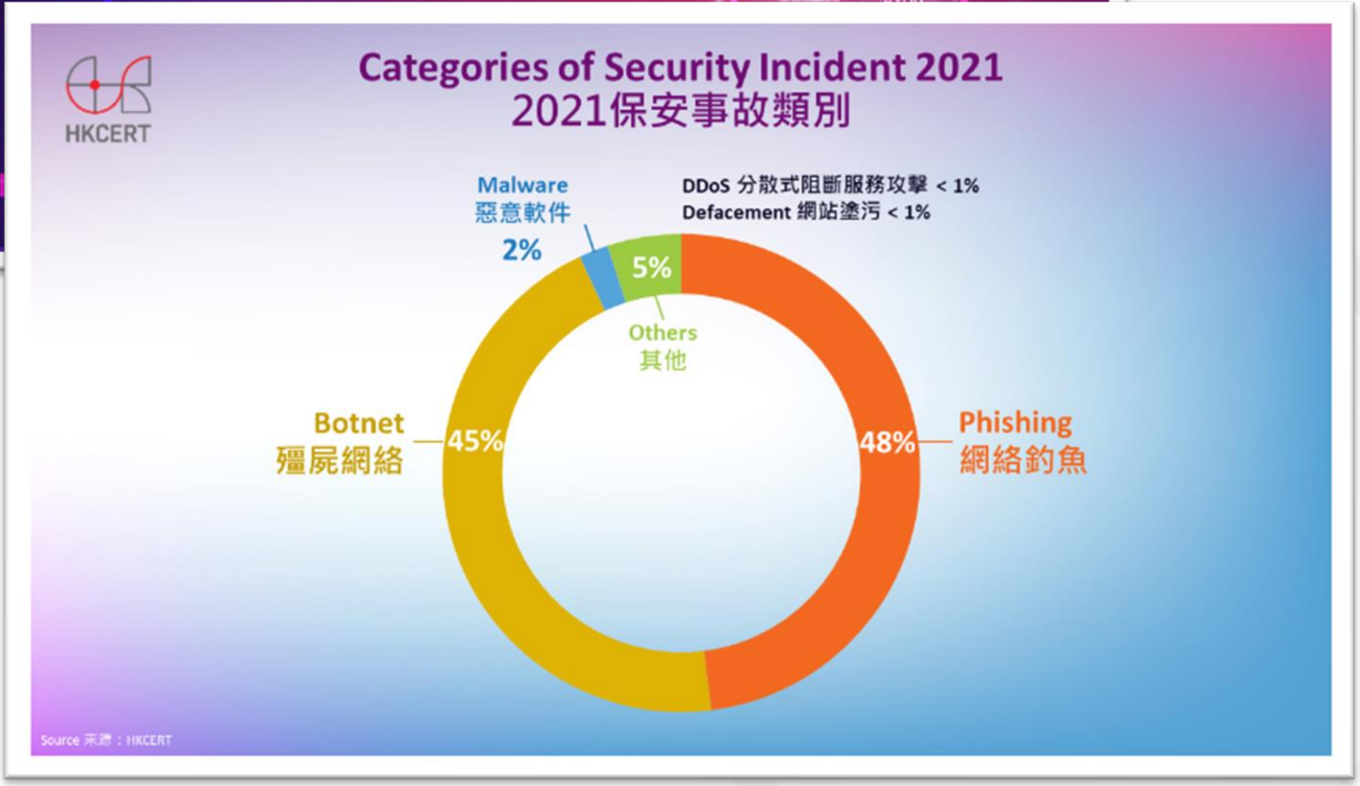
Phishing – Major Security Incident in 2021



網絡攻擊趨複雜及多元化 網絡釣魚事故創新高 HKCERT 呼籲全民資訊保安意識要提高

香港生產力促進局（生產力局）轄下的香港電腦保安事故協調中心 （HKCERT）今日總結 2021 年香港資訊保安狀況並發布 2022 年保安預測。過去一年，疫情仍然肆 虐，大大改變了企...

了解更多

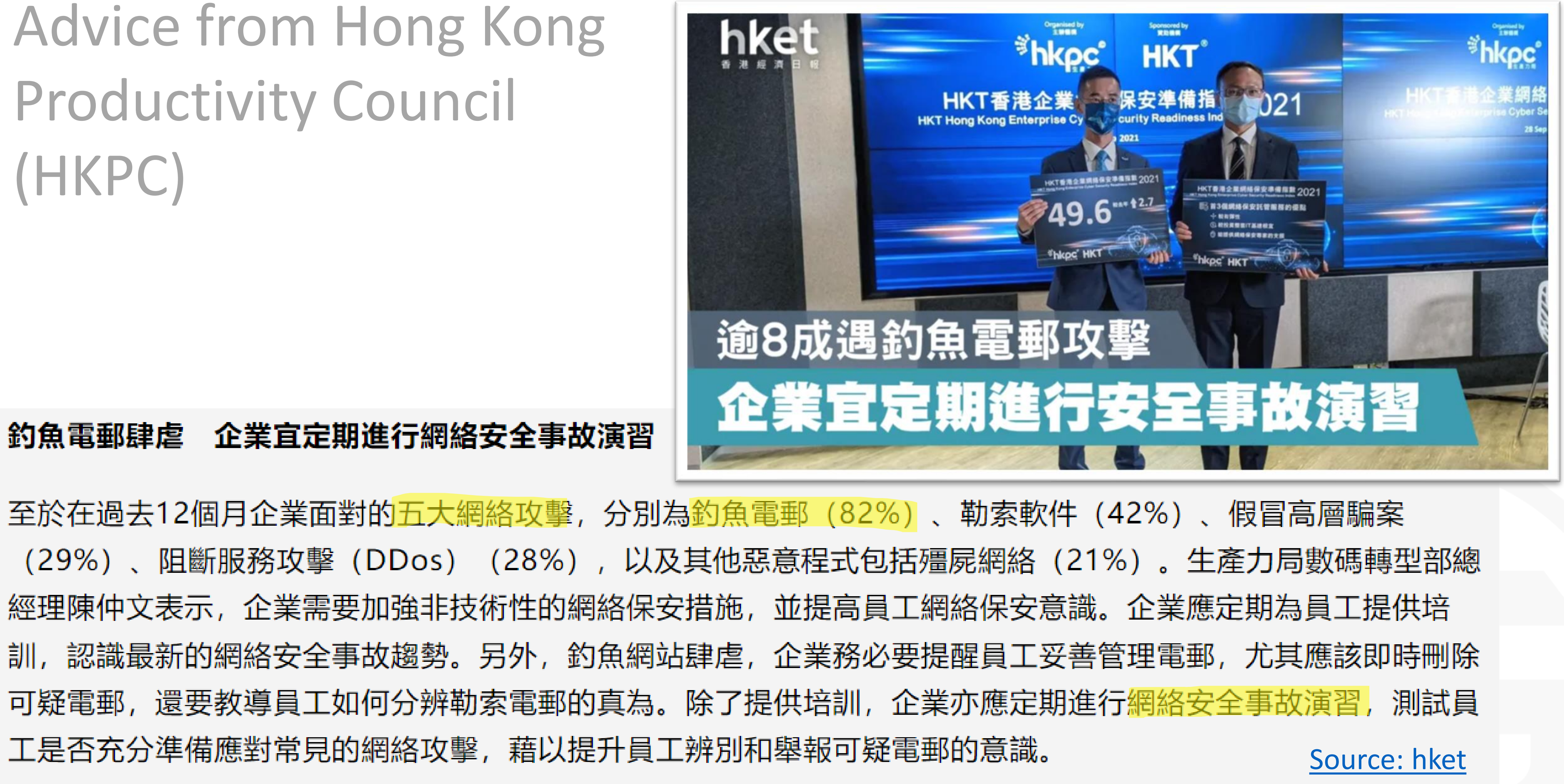


Categories of Security Incident 2021
2021保安事故類別

Source 來源：HKCERT

Full article on HKCERT website

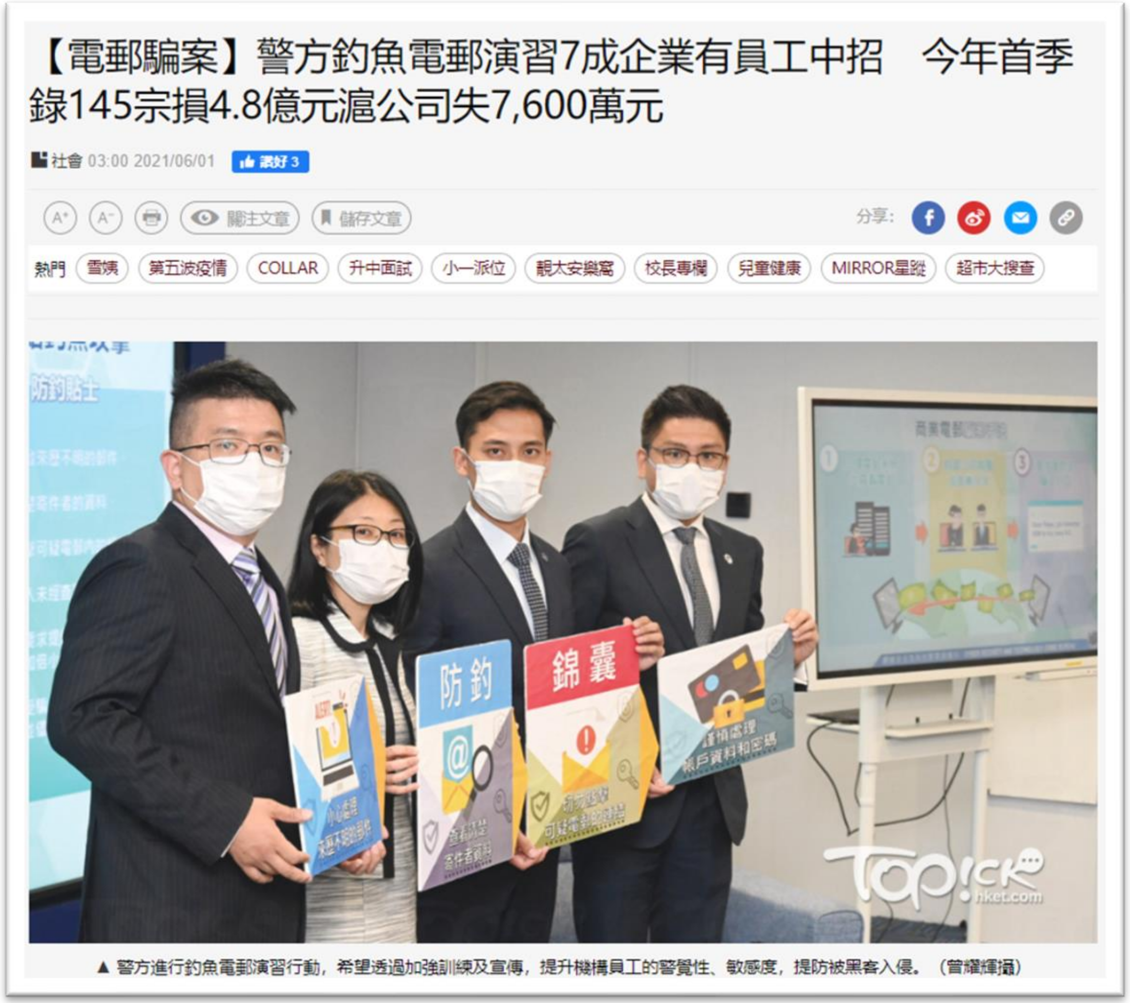
Advice from Hong Kong Productivity Council (HKPC)


hket
香港經濟日報
hkpc
HKT
HKT香港企業網絡保安準備指數2021
HKT Hong Kong Enterprise Cyber Security Readiness Index 2021
49.6
2.7
逾8成遇釣魚電郵攻擊
企業宜定期進行安全事故演習

釣魚電郵肆虐　企業宜定期進行網絡安全事故演習

至於在過去12個月企業面對的五大網絡攻擊，分別為釣魚電郵（82%）、勒索軟件（42%）、假冒高層騙案（29%）、阻斷服務攻擊（DDos）（28%），以及其他惡意程式包括殭屍網絡（21%）。生產力局數碼轉型部總經理陳仲文表示，企業需要加強非技術性的網絡保安措施，並提高員工網絡保安意識。企業應定期為員工提供培訓，認識最新的網絡安全事故趨勢。另外，釣魚網站肆虐，企業務必要提醒員工妥善管理電郵，尤其應該即時刪除可疑電郵，還要教導員工如何分辨勒索電郵的真偽。除了提供培訓，企業亦應定期進行網絡安全事故演習，測試員工是否充分準備應對常見的網絡攻擊，藉以提升員工辨別和舉報可疑電郵的意識。

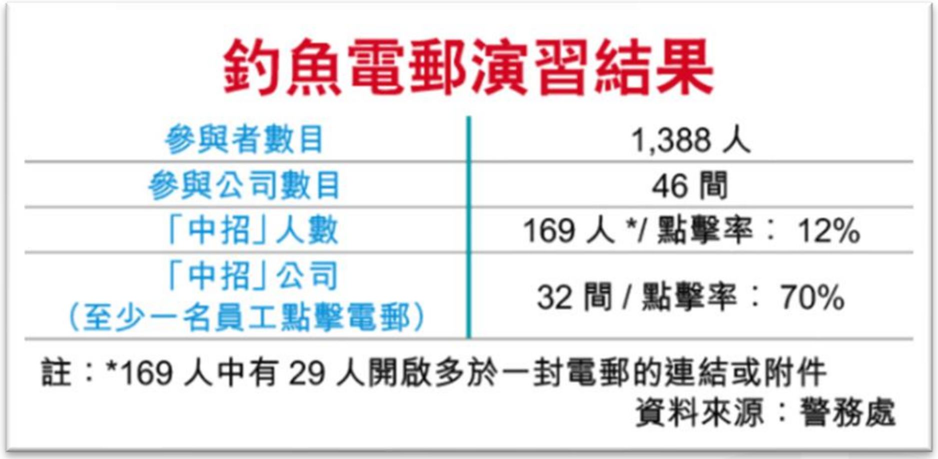
Source: hket



【電郵騙案】警方釣魚電郵演習7成企業有員工中招　今年首季錄145宗損4.8億元滬公司失7,600萬元

社會 03:00 2021/06/01

▲ 警方進行釣魚電郵演習行動，希望透過加強訓練及宣傳，提升機構員工的警覺性、敏感度，提防被黑客入侵。（管耀輝攝）



釣魚電郵演習結果

參與者數目	1,388 人
參與公司數目	46 間
「中招」人數	169 人 */ 點擊率： 12%
「中招」公司 （至少一名員工點擊電郵）	32 間 / 點擊率： 70%

註：*169 人中有 29 人開啟多於一封電郵的連結或附件

資料來源：警務處

警方認為其中一個有效提防電郵騙案的方法，是提升大眾分辨可疑電郵的敏感度。網罪科4月初舉辦了釣魚電郵演習，邀請46家銀行、公營機構等界別，共逾1,388人參與，當中32間公司至少有一名員工中招。網罪科網絡安全組總督察葉卓譽稱，逾三分一中招者點擊「雲端文件分享」的電郵，「疫苗接種」及「稅務退還」也各佔2成多，情況與外國同類調查相若，顯示如騙案涉及社會熱話，更易令人受騙：「員工已事先知悉有演習，否則情況可能更差」。

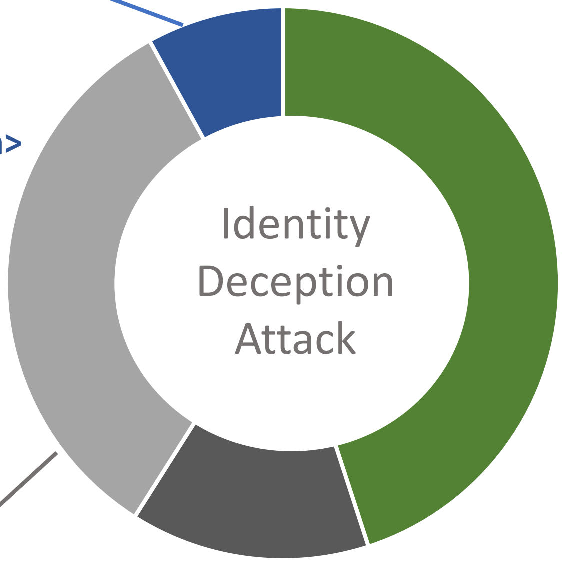
Source: Topick

Common Attack Samples

Phishing attacks commonly seen in HK NGO environment

Typical Scenarios of Phishing - Impersonation

Attack Category



8%
Compromised Account

From: Purchasing - Roy Lim <rlim@abcNGO.com>
To: Finance - Cherry Ho <cho@abcNGO.com>
Subject: 付款通知 - PO 382313

45%
Display Name Deception (Brand)

From: Pay-Me <payme-hsbc@gmail.com>
To: TM Chan <taiman.chan@AbcNGO.com>
Subject: 您的PayMe賬戶收到一筆款項！請盡快按此收款

33%
Display Name Deception (Individual)

From: CEO – David TM Chan <CEO@abcNGO.com>
To: Richard C Lee <CFO@abcNGO.com>
Subject: Follow Up on Invoice Payment

14%
Look-alike Domain

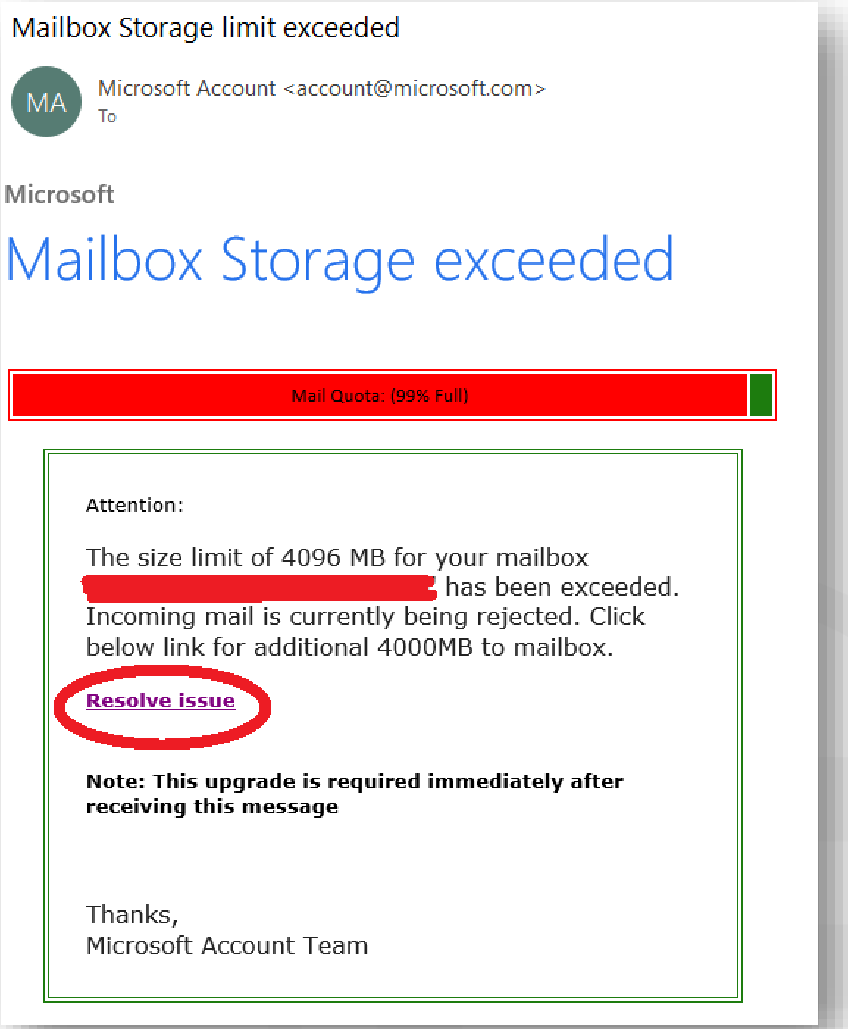
From: LinkedIn <noreply@1inkedin.com>
To: TM Chan <taiman.chan@abcNGO.com>
Subject: Diana 在一則貼文標記了你! 按此登入以查看。

Phishing Example – Fake Microsoft Warning

Common Case Scenario:

- Hacker used any excuse and asked staff to click the **phishing URL**.
- Victim being directed to a phishing website and asked to enter his/her company email address and **password**.
- Hacker took over (**compromised**) victim's company email account.
  - **Internal:** leverage the **stolen** account to send **malicious** emails (e.g., phishing, ransomware) to **infect other colleagues**.
  - **External:** study the **email communication** of the compromised account and send phishing emails to **other NGOs.**
- **Related NGOs would be the next victim** especially if they set the compromised NGO as **"Trusted Sender" unless** they have **email security protection for Advanced Phishing protection.**

- **Potential Consequences**:
  - Damage on Reputation,
  - Financial Loss
  - Company Privacy / Confidential Data Loss…



Mailbox Storage limit exceeded

MA Microsoft Account <account@microsoft.com>
To

Microsoft

Mailbox Storage exceeded

Mail Quota: (99% Full)

Attention:

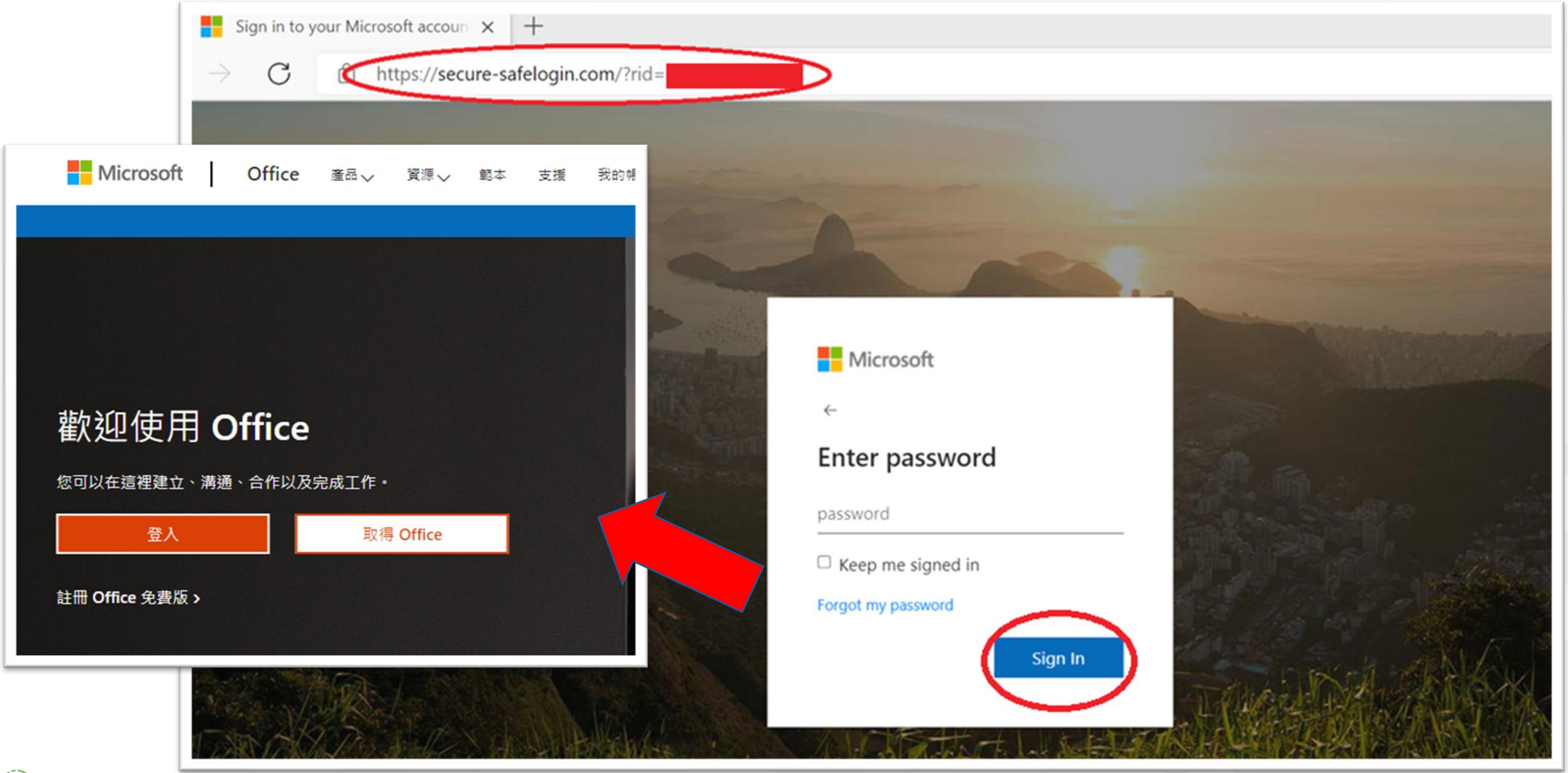
The size limit of 4096 MB for your mailbox [redacted] has been exceeded. Incoming mail is currently being rejected. Click below link for additional 4000MB to mailbox.

Resolve issue

Note: This upgrade is required immediately after receiving this message

Thanks,
Microsoft Account Team

Phishing Example – Hacker trying to steal staff’s Microsoft Login Password



Sign in to your Microsoft accoun

https://secure-safelogin.com/?rid=[redacted]

歡迎使用 Office

您可以在這裡建立、溝通、合作以及完成工作。

Enter password

password

□ Keep me signed in

Security Challenges

No Zero-Day Malware detection

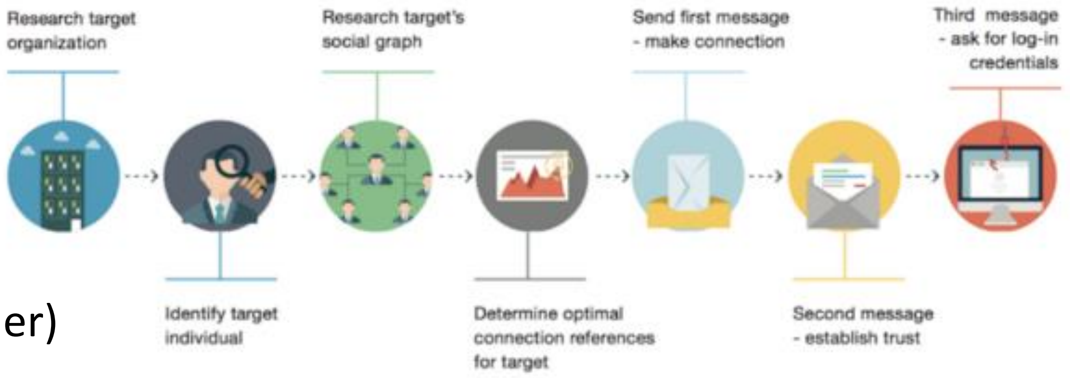
- Traditional anti-virus engine cannot detect Zero-Day Malware. Free mailbox service doesn’t include advanced protection like Sandboxing for free.

Inefficient URL analysis

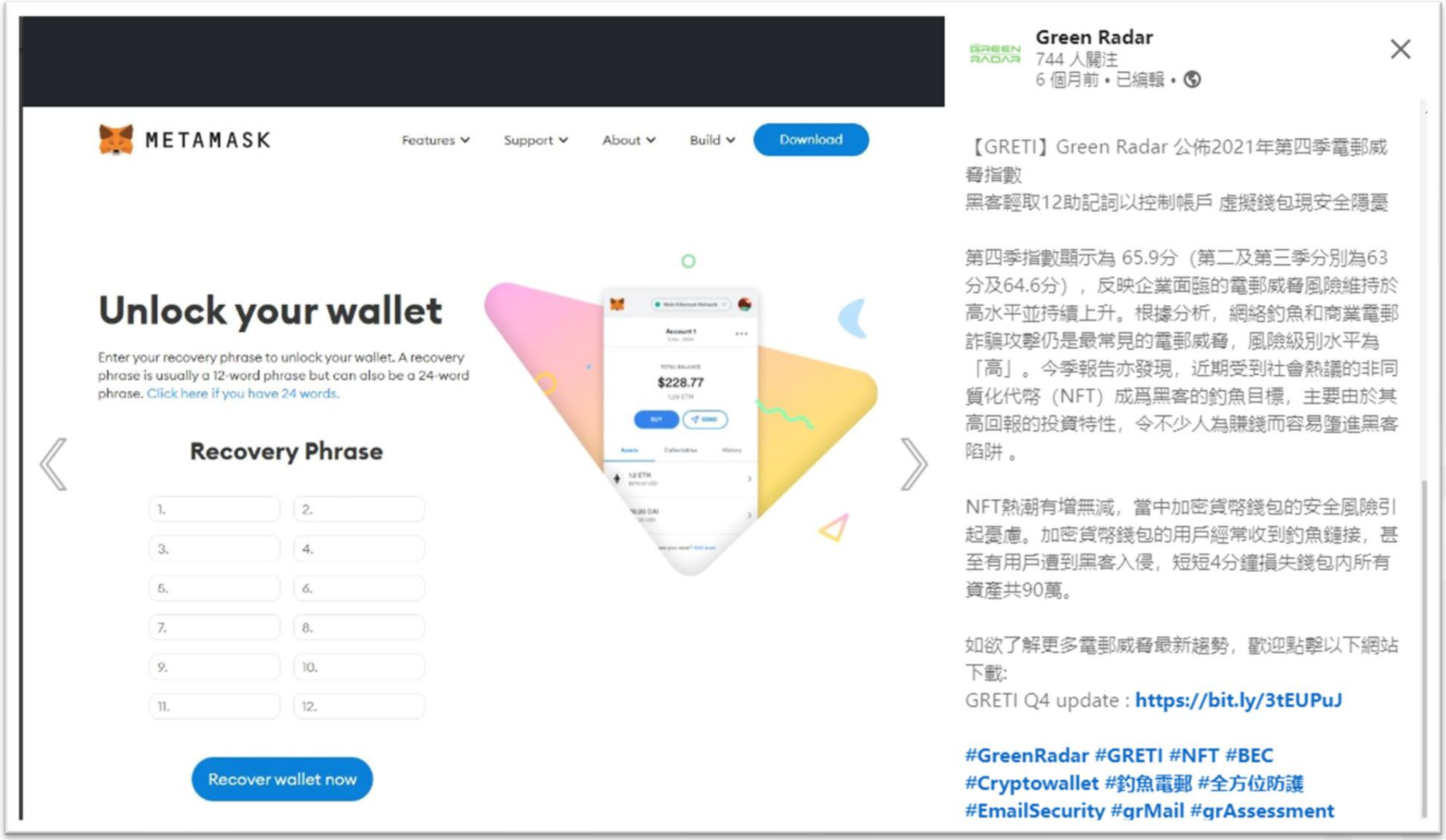
- Zero-Day phishing URL cannot be blocked by traditional anti-spam engine.

Targeted phishing

- Pretend from a trusted source
  - (e.g., your NGO domain/staff/ Other NGO Partner)
- May not have malware/phishing link
  - (e.g., VIP spoofing)


Research target organization
Identify target individual
Research target's social graph
Determine optimal connection references for target
Send first message - make connection
Second message - establish trust
Third message - ask for log-in credentials

Follow Green Radar Social Media Page for Latest Attack Update



Unlock your wallet

Enter your recovery phrase to unlock your wallet. A recovery phrase is usually a 12-word phrase but can also be a 24-word phrase. Click here if you have 24 words.

Recovery Phrase

1. 2.
3. 4.
5. 6.
7. 8.
9. 10.
11. 12.

Green Radar
744 人關注
6 個月前 • 已編輯 •

【GRETI】Green Radar 公佈2021年第四季電郵威脅指數
黑客輕取12助記詞以控制帳戶 虛擬錢包現安全隱憂

第四季指數顯示為 65.9分（第二及第三季分別為63分及64.6分），反映企業面臨的電郵威脅風險維持於高水平並持續上升。根據分析，網絡釣魚和商業電郵詐騙攻擊仍是最常見的電郵威脅，風險級別水平為「高」。今季報告亦發現，近期受到社會熱議的非同質化代幣（NFT）成爲黑客的釣魚目標，主要由於其高回報的投資特性，令不少人為賺錢而容易墮進黑客陷阱 。

NFT熱潮有增無減，當中加密貨幣錢包的安全風險引起憂慮。加密貨幣錢包的用戶經常收到釣魚鏈接，甚至有用戶遭到黑客入侵，短短4分鐘損失錢包內所有資產共90萬。

如欲了解更多電郵威脅最新趨勢，歡迎點擊以下網站下載:
GRETI Q4 update : https://bit.ly/3tEUPuJ

#GreenRadar #GRETI #NFT #BEC
#Cryptowallet #釣魚電郵 #全方位防護
#EmailSecurity #grMail #grAssessment

Scan here for Green Radar

Scan here for Green Radar

Total Solution: grMail + grAssessment

Technology available in the Market
to protect your organization from phishing attack

Continuous email security improvement with **two key solutions**

grMail™

Green Radar offers comprehensive email protection via our proprietary aidar™ technology that is delivered and managed by a team of security experts in our dedicated Security Operations Center in Hong Kong and Singapore. We are working around the clock to dynamically scan and remove threats on every email before it reaches your inbox.

aidar™
AI | Detection | Analytics | Response

THREATS DETECTION

grAssessment

grAssessment is a program to support our customers to improve cybersecurity awareness and practices by conducting customized phishing assessment campaigns. It reassurances customers with a peace of mind that their workforce has a heightened sense of awareness to help protect their organizations from phishing attacks.

USER COLLABORATION

grMail Block malicious emails before they reach your staff's inbox

Phishing is a **major Cyberattack incident** in HK according to HKCERT
Green Radar grMail is one of the popular solution to protect staff from **Phishing Attacks**.

Protect you from

✓ **Hyperlink attack** (direct employee to phishing website)

✓ **Attachment attack** (virus/zero-day ransomware)

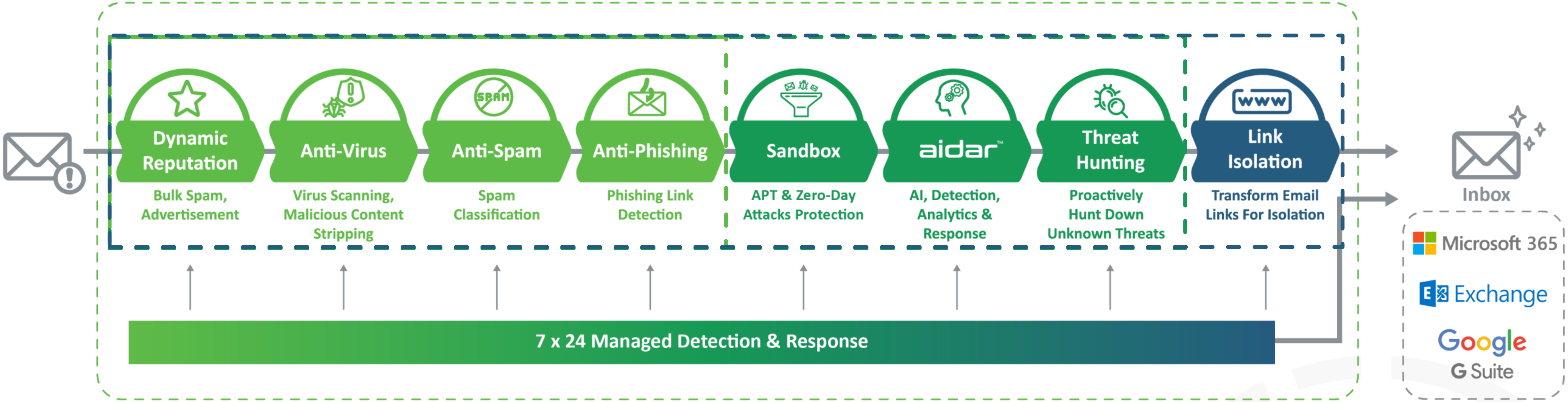
✓ **Advanced phishing** (e.g., Attack pretending to be sent from someone@abcNGO.org.hk / NGO partners which contains **no phishing link/malware** and hard to be detected through traditional signature-based technology, e.g., AV/AS)

Operation-wise

- User friendly: SOC Managed service reduces NGO IT admin workload
- Support Service : 7x24 Local Response (available in Cantonese/ English)

GREEN RADAR
Redefining Email Security

grMail



Dynamic Reputation
Bulk Spam, Advertisement
Anti-Virus
Virus Scanning, Malicious Content Stripping
Anti-Spam
Spam Classification
Anti-Phishing
Phishing Link Detection
Sandbox
APT & Zero-Day Attacks Protection
aidar™
AI, Detection, Analytics & Response
Threat Hunting
Proactively Hunt Down Unknown Threats
Link Isolation
Transform Email Links For Isolation
7 x 24 Managed Detection & Response
Inbox
Microsoft 365
Exchange
Google
G Suite

grMail Professional

All except “Link Isolation”

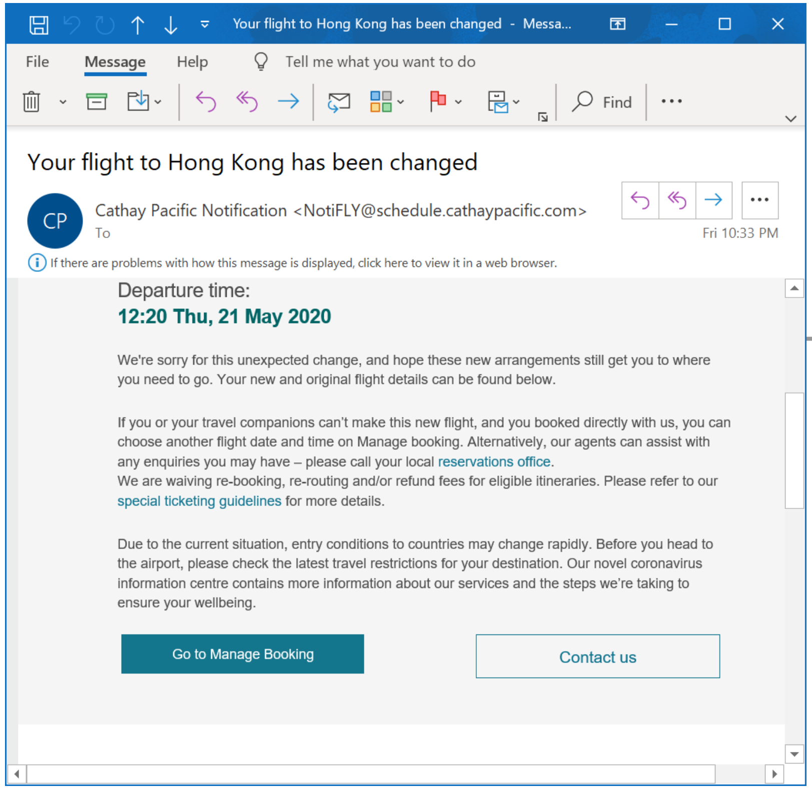
grMail Advanced

“grMail Professional” plus:

- Link isolation
  (protect staff from attack via online document, e.g., SharePoint / OneDrive)

GREEN RADAR
Redefining Email Security

Link Isolation – Classify website and protect staff from clicking through phishing website


Your flight to Hong Kong has been changed - Messa...
File
Message
Help
Tell me what you want to do
Find

Your flight to Hong Kong has been changed

Cathay Pacific Notification <NotiFLY@schedule.cathaypacific.com>
To
Fri 10:33 PM

If there are problems with how this message is displayed, click here to view it in a web browser.

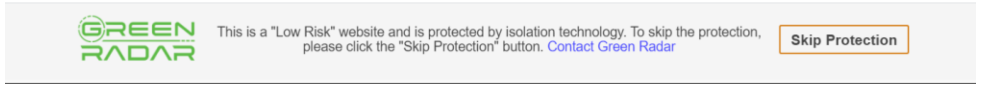
Departure time:
12:20 Thu, 21 May 2020

We're sorry for this unexpected change, and hope these new arrangements still get you to where you need to go. Your new and original flight details can be found below.

If you or your travel companions can't make this new flight, and you booked directly with us, you can choose another flight date and time on Manage booking. Alternatively, our agents can assist with any enquiries you may have – please call your local reservations office.
We are waiving re-booking, re-routing and/or refund fees for eligible itineraries. Please refer to our special ticketing guidelines for more details.

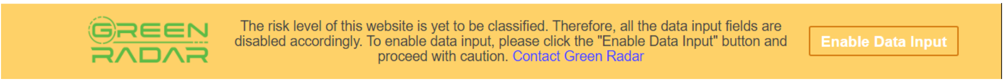
Due to the current situation, entry conditions to countries may change rapidly. Before you head to the airport, please check the latest travel restrictions for your destination. Our novel coronavirus information centre contains more information about our services and the steps we're taking to ensure your wellbeing.

Low Risk Website



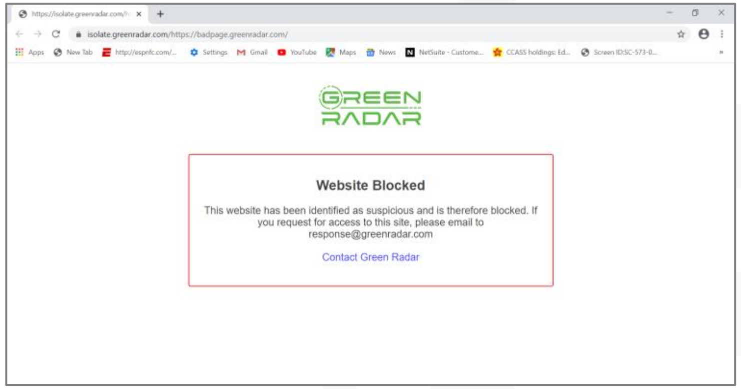
This is a "Low Risk" website and is protected by isolation technology. To skip the protection, please click the "Skip Protection" button. Contact Green Radar

Cautious Website



The risk level of this website is yet to be classified. Therefore, all the data input fields are disabled accordingly. To enable data input, please click the "Enable Data Input" button and proceed with caution. Contact Green Radar

Phishing Website



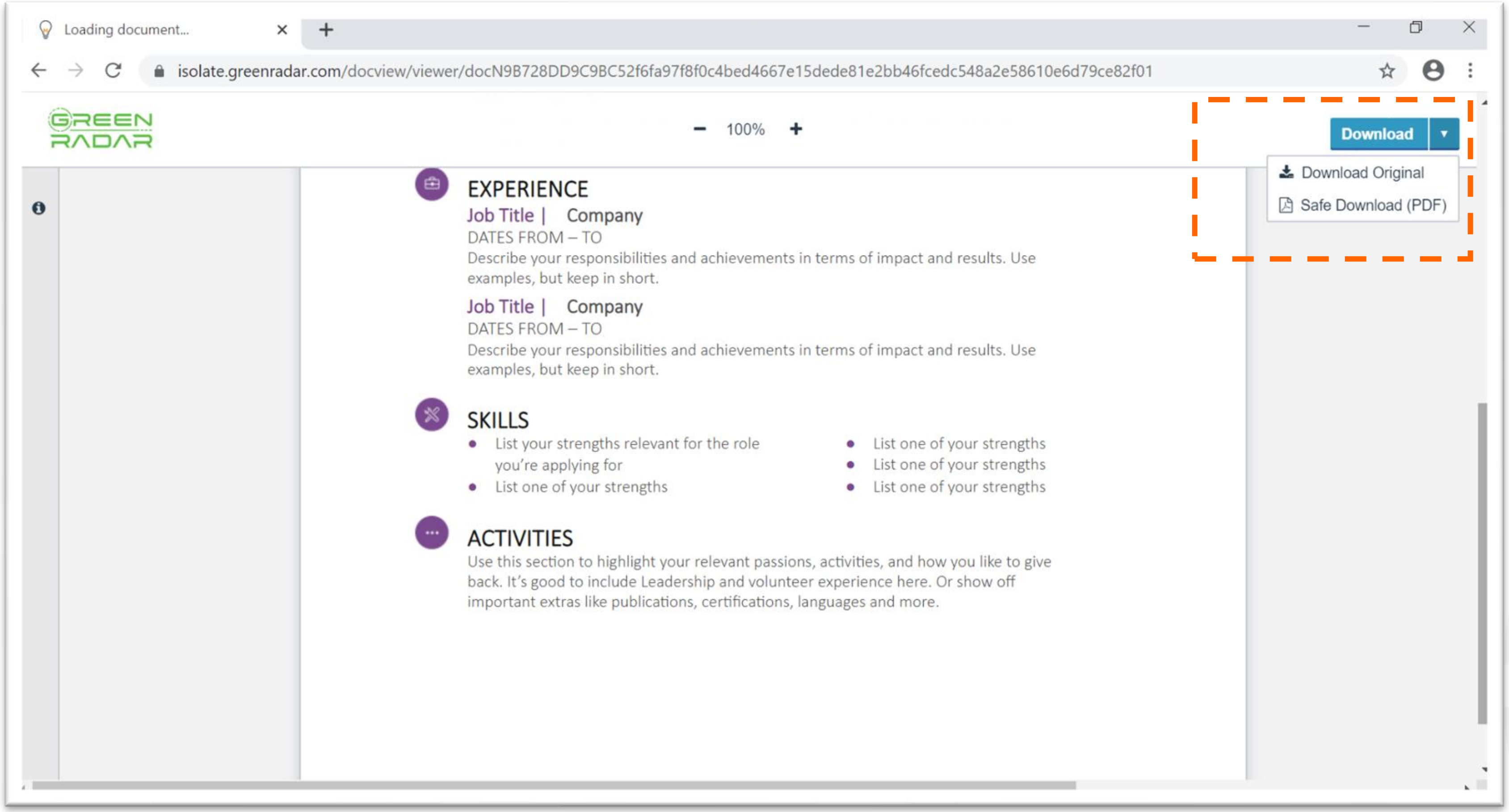
Website Blocked

This website has been identified as suspicious and is therefore blocked. If you request for access to this site, please email to response@greenradar.com

Contact Green Radar

Link Isolation – Malware-free Document Viewing e.g., SharePoint, One Drive, Google Drive, etc.

Many cyberattacks are disguised as ordinary online documents e.g., CV / quotation / invoice to trap staff



Loading document...
isolate.greenradar.com/docview/viewer/docN9B728DD9C9BC52f6fa97f8f0c4bed4667e15dede81e2bb46fcedc548a2e58610e6d79ce82f01
GREEN RADAR
100%
Download
Download Original
Safe Download (PDF)

EXPERIENCE

Job Title | Company

DATES FROM – TO

Describe your responsibilities and achievements in terms of impact and results. Use examples, but keep in short.

Job Title | Company

DATES FROM – TO

Describe your responsibilities and achievements in terms of impact and results. Use examples, but keep in short.

SKILLS

- List your strengths relevant for the role you're applying for
- List one of your strengths
- List one of your strengths
- List one of your strengths
- List one of your strengths

ACTIVITIES

Use this section to highlight your relevant passions, activities, and how you like to give back. It's good to include Leadership and volunteer experience here. Or show off important extras like publications, certifications, languages and more.

Support PDF conversion (100% malware-free Safe Download) & Original Download

Example: Potentially harmful online CV targeting HR department. Isolation technology removes malicious elements in the document and ensure safe browsing

GREEN RADAR
Redefining Email Security

Green Radar & Microsoft 365 / Google

What protection we can add on top of your existing Microsoft / Google mailbox

grMail™ brings additional protection on top of your Microsoft /Google inbox

Functions	Microsoft Mailbox EOP (Free and Common)	Microsoft Defender Plan 1 OR 2 (additional $$)	Google Mailbox Default Setting	Green Radar grMail Professional (Popular solution among NGOs in HK)
1. Identify Known Phishing URL	No	Yes, Safe Link feature (**Static URL checking**).	Move to Junk Box. No quarantine.	Yes. Uses **Sandboxing Approach** to analyze **Dynamic** behavior of the URL (URL Sandboxing)
2. Identify Zero Day Phishing URL	No	No. Static URL checking cannot detect Zero Day Phishing URL	No quarantine.	Yes. Uses Sandboxing Approach to analyze **Dynamic** behavior of the URL (URL Sandboxing)
3. Identify Zero Day Malware in attachments	No	Yes, Safe Attachment feature	No quarantine.	Yes. **Local Sandboxing** ensures speed, performance and accessibility from China / Hong Kong users.
4. Prevent Domain Spoofing Fake email sent from "someone@abcNGO.org.hk"	No	No	No quarantine.	Yes. Provides SPF* checking at header level. With look alike domain AI analysis.
5. Prevent VIP Spoofing Fake email sent from the name of management	No	No	No quarantine.	Yes. Provides VIP watchlist and SOC service for proactive VIP anomaly investigation.
6. Prevent BEC* attack Pure-text scam email that contains no URL / attachments	No	No	No quarantine.	Yes. Provides AI Detection and Investigation for indicator of compromises, e.g., "reply-to inconsistency" ,in addition to email content / URL / attachment detection.

*SPF: Sender Policy Framework
*BEC: Business Email Compromised

grAssessment

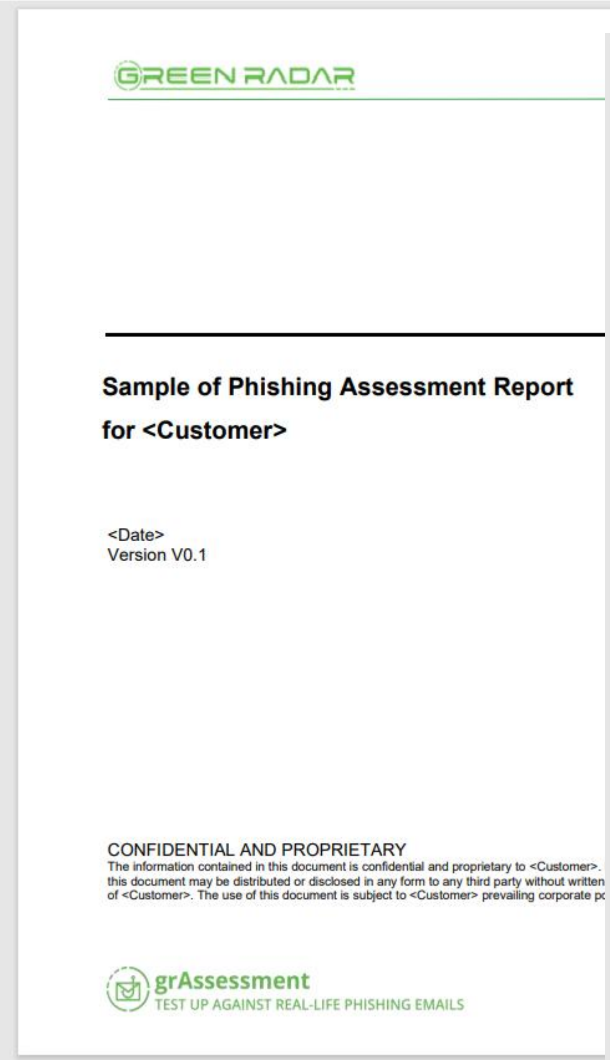
- phishing assessment campaign to enhance user awareness

Data statistic to be collected

	Initialize	1st Click	2nd Click	3rd Click	Result
Phishing Link	⚪	🔵	🟠	Submit Credential	Credential Leaked
Malware Download Link	⚪	🔵	🟠	Download Attachment	Malware Downloaded
Malware Attachment	⚪	🔵	🟠	Open Attachment	Malware Installed
BEC	⚪			Respond to Email	🔴

⚪ Delivered to inbox 🔵 Open Email 🟠 Open Link / Attachment 🔴 Compromised

Sample Management Report



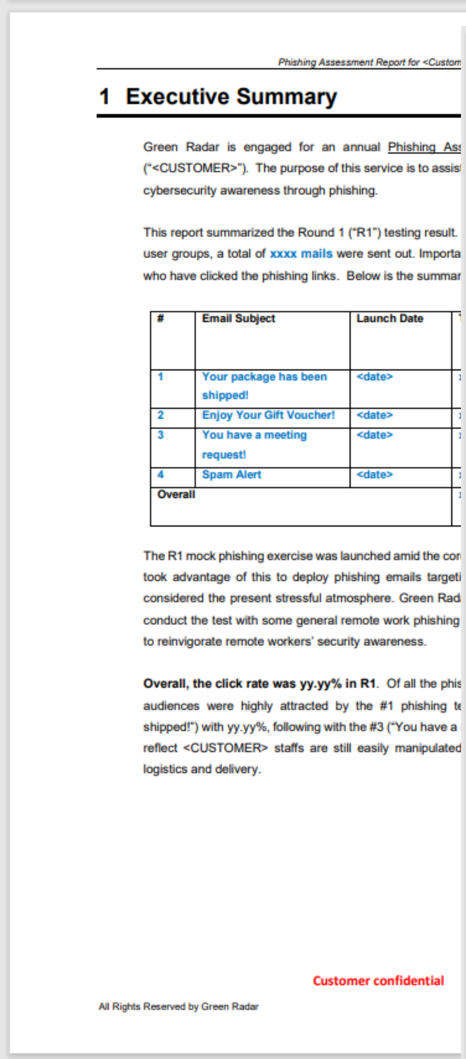
GREEN RADAR

Sample of Phishing Assessment Report for <Customer>

<Date>
Version V0.1

CONFIDENTIAL AND PROPRIETARY
The information contained in this document is confidential and proprietary to <Customer>.
this document may be distributed or disclosed in any form to any third party without written
of <Customer>. The use of this document is subject to <Customer> prevailing corporate p

grAssessment
TEST UP AGAINST REAL-LIFE PHISHING EMAILS



Phishing Assessment Report for <Custom

1 Executive Summary

Green Radar is engaged for an annual Phishing As
("<CUSTOMER>"). The purpose of this service is to assis
cybersecurity awareness through phishing.

This report summarized the Round 1 ("R1") testing result.
user groups, a total of xxxx mails were sent out. Importa
who have clicked the phishing links. Below is the summar

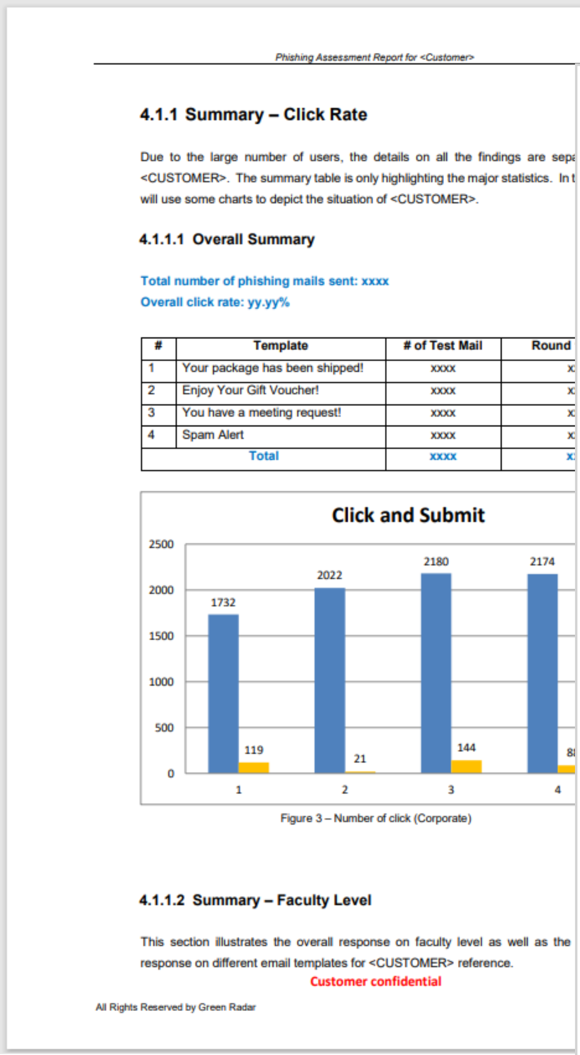
#	Email Subject	Launch Date
1	Your package has been shipped!	<date>
2	Enjoy Your Gift Voucher!	<date>
3	You have a meeting request!	<date>
4	Spam Alert	<date>
Overall		

The R1 mock phishing exercise was launched amid the co
took advantage of this to deploy phishing emails targeti
considered the present stressful atmosphere. Green Rad
conduct the test with some general remote work phishing
to reinvigorate remote workers' security awareness.

Overall, the click rate was yy.yy% in R1. Of all the phis
audiences were highly attracted by the #1 phishing t
shipped!") with yy.yy%, following with the #3 ("You have a
reflect <CUSTOMER> staffs are still easily manipulated
logistics and delivery.

Customer confidential

All Rights Reserved by Green Radar



Phishing Assessment Report for <Customer>

4.1.1 Summary – Click Rate

Due to the large number of users, the details on all the findings are sep
<CUSTOMER>. The summary table is only highlighting the major statistics. In t
will use some charts to depict the situation of <CUSTOMER>.

4.1.1.1 Overall Summary

Total number of phishing mails sent: xxxx
Overall click rate: yy.yy%

#	Template	# of Test Mail	Round
1	Your package has been shipped!	xxxx	x
2	Enjoy Your Gift Voucher!	xxxx	x
3	You have a meeting request!	xxxx	x
4	Spam Alert	xxxx	x
	Total	xxxx	x

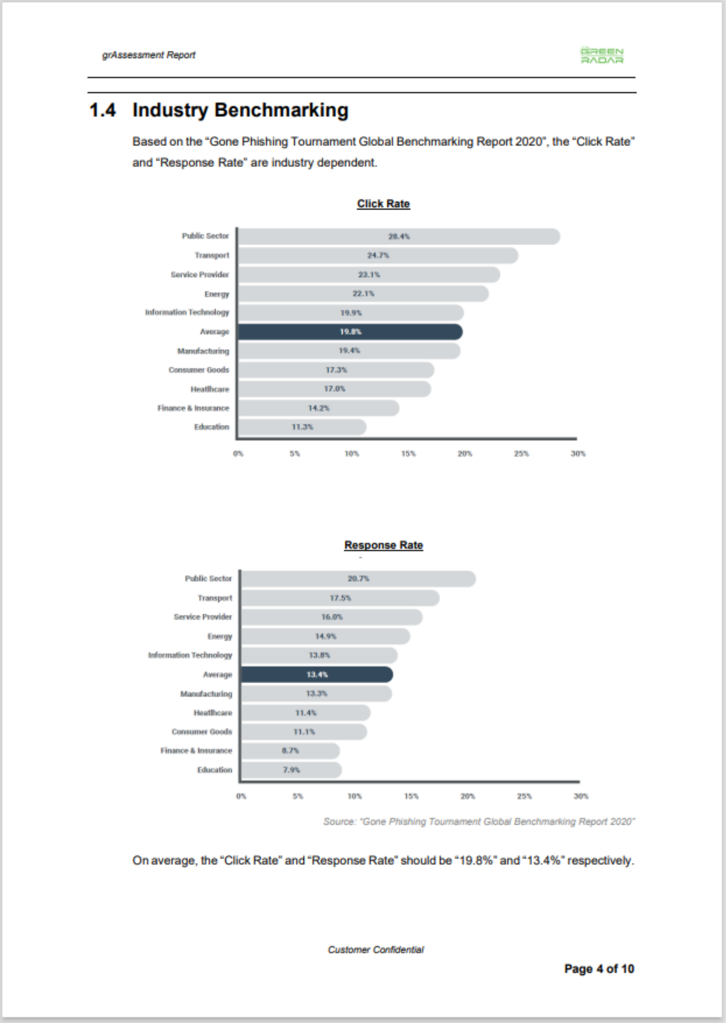
Figure 3 – Number of click (Corporate)

4.1.1.2 Summary – Faculty Level

This section illustrates the overall response on faculty level as well as the
response on different email templates for <CUSTOMER> reference.

Customer confidential

All Rights Reserved by Green Radar



grAssessment Report

1.4 Industry Benchmarking

Based on the "Gone Phishing Tournament Global Benchmarking Report 2020", the "Click Rate" and "Response Rate" are industry dependent.

Source: "Gone Phishing Tournament Global Benchmarking Report 2020"

On average, the "Click Rate" and "Response Rate" should be "19.8%" and "13.4%" respectively.

Customer Confidential

Page 4 of 10

GREEN RADAR
Redefining Email Security

Real time educational video to refresh awareness

應對釣魚
電郵基本功
NAME
From: sales@microsoft.com
檢查方法
(一)
留意網址預覽
小心假冒朋友

Green Radar: Track and collect view statistics

Remarks:

- Video is also available in English language
- Traditional / Simplified Chinese Subtitle available

Green Radar's approach to
Phishing Assessment Program

PROFESSIONAL

Managed by Certified Cybersecurity professionals

SIMULATIONS

Emulate real world phishing simulations like a hacker

TRAINING

Real-time bite-sized training when problem arises

MONITORING

Regular and disciplined pulse checks

GREEN RADAR
Redefining Email Security

No longer challenges with grMail and grAssessment

24 x 7 Expertise Support

Fully affordable

Expertise Consultancy

Proactive Response

Green Radar Company Background

– wholly owned subsidiary of

edvance Edvance International Holdings Limited (HKEx: 1410)

Green Radar – Hong Kong-based Email Security Service Provider

20+

years CyberSecurity experience

No. 1

HK Cybersecurity Distributor

- ✓6,000 ft² office in HK for Security Operations Center (SOC)
- ✓2 x data centers in HK (Local sandboxing✓)
- ✓2 x SOCs in HK & SG
- ✓Provides local threat hunting & support services
- ✓Equip with R&D team for technology control & development

GREEN RADAR
Redefining Email Security

Green Radar – Unique Security-as-a-Service Vendor

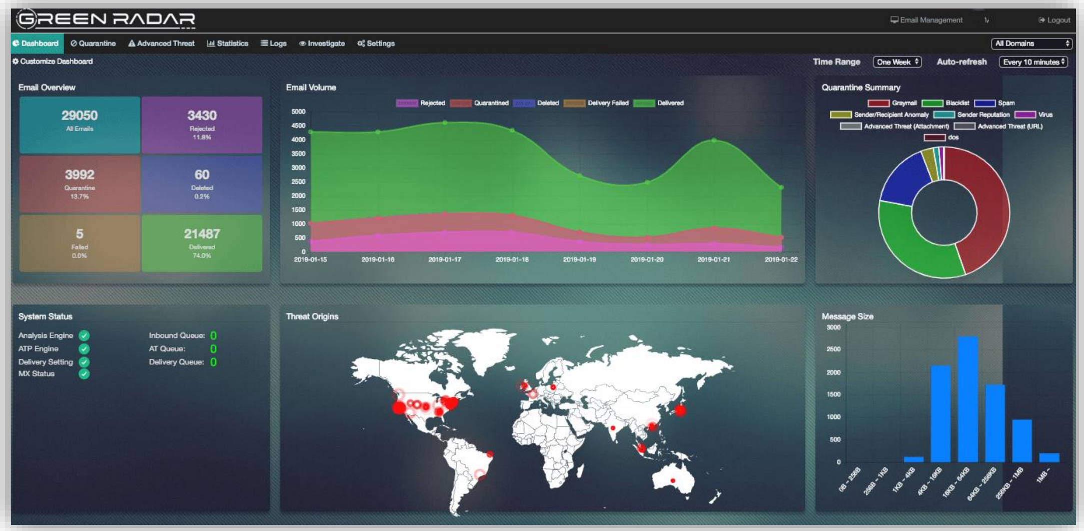
Local Technology

R&D experts

Local SOC

Local support expertise

Self developed AI engine



All Domains

Time Range: One Week

Auto-refresh: Every 10 minutes

Email Overview

29050 All Emails	3430 Rejected 11.8%
3992 Quarantine 13.7%	60 Deleted 0.2%
5 Failed 0.0%	21487 Delivered 74.0%

System Status

Analysis Engine ✓

ATP Engine ✓

Delivery Setting ✓

MX Status ✓

Inbound Queue: 0

AT Queue: 0

Delivery Queue: 0

Hong Kong | Singapore

GREEN RADAR
Redefining Email Security

Green Radar SOC Team continuously providing Email Support Service to Top HK Enterprise and Government Departments

HONG KONG MONETARY AUTHORITY
香港金融管理局

HKEX
香港交易所

SECURITIES AND FUTURES COMMISSION
證券及期貨事務監察委員會

香港特別行政區政府
房屋署

創興銀行
Chong Hing Bank

SONY

HKMC
香港按揭證券有限公司
The Hong Kong Mortgage Corporation Limited

海通國際
HAITONG

煤氣
Towngas
環保生活每一天
Go Green Every Day

機電工程署
EMSD
香港特別行政區政府
機電工程署

中國銀行(香港)
BANK OF CHINA (HONG KONG)
信用卡
Credit Card

HUTCHISON PORTS
HIT

香港特別行政區政府
香港警務處
忠誠勇毅 心繫社會

MUFG

A.S. Watson Group
A member of CK Hutchison Holdings
180 YEARS OF love
Since 1841
A.S. Watson Group

Green Radar Customers (Commercial)

MUJI
無印良品

759 Store
759阿信屋

和記地產集團有限公司
HUTCHISON PROPERTY GROUP LIMITED
(A limited liability British Virgin Islands company registered in Hong Kong)
Member of Cheung Kong Property Group

SHK
新鴻基地產
Sun Hung Kai Properties

FANCL

city'super

中國建築國際集團有限公司
CHINA STATE CONSTRUCTION INTERNATIONAL HOLDINGS LIMITED
（於開曼群島註冊成立之有限公司）
(Incorporated in the Cayman Islands with limited liability)

BCT
銀聯集團

Jardine Aviation Services
怡中航空服務

農銀國際
ABC INTERNATIONAL

TW
翠華集團
Tsui Wah Group

TWG 捷榮集團

KORCHINA Logistics Solution

AJS
安捷證券

PRINCE太子
珠寶鐘錶 JEWELLERY & WATCH

DR·KONG

元泰集團
Orient Star Group

CASH 時富

Pricerite實惠

FUJIFILM
Value from Innovation

GLS

HONG KONG COUNTRY CLUB
香港鄉村俱樂部

mfJebsen

tom

GREEN RADAR
Redefining Email Security

Assurance to our customers

Guarantee **99.999%** availability (we achieved 100% uptime in the past 3 years)

Email processing time less than **10s** without attachment

SPAM capture rate

> **99%**

Awards & Recognition

- eZone eBrand Award 2020 – The Best Email Security Solution
- PCM Biz.IT Excellence 2021 – IT Solution Excellence
- APAC CIO Outlook Top 10 Cyber Security Companies 2021
- 2021 CybersecAsia Readers Choice Awards – Rising Star

GREEN RADAR

Reliable Protection Against Cyber Threats

THANK YOU!

Green Radar (Hong Kong) Limited
18/F, 9 Chong Yip Street, Kwun Tong,
Kowloon, Hong Kong
T: +852 3194 2200

Green Radar (Singapore) Pte. Ltd.
2 Sims Close #01-11/12
Gemini@Sims Singapore 387298
T: +65 6248 0600

info@greenradar.com
www.greenradar.com
a member of Edvance International (1410.HK)