

Cybersecurity in Healthcare

醫療保健業的網絡安全

Fuller Yu

Chief Information Security Officer, Hospital Authority
Co-Chair of Cyber Security Work Stream, Global Digital
Health Partnership (GDHP)

October 2021

Healthcare Industry is an attractive target of cyber attacks

“Low hanging fruit” target



High value of patient records



Scarce cybersecurity resources



Increasing digital transformation



Cybersecurity Challenge in Healthcare Organisation



Cybersecurity Challenge in Healthcare Organisation



- ▶ Huge volume of medical data need to be protected
- ▶ Extended data exchange with increased third parties



- ▶ Clinical IT systems as mission critical
- ▶ Medical devices with inadequate security controls
- ▶ Risks of emerging technologies (Cloud, AI, 5G, Big Data)

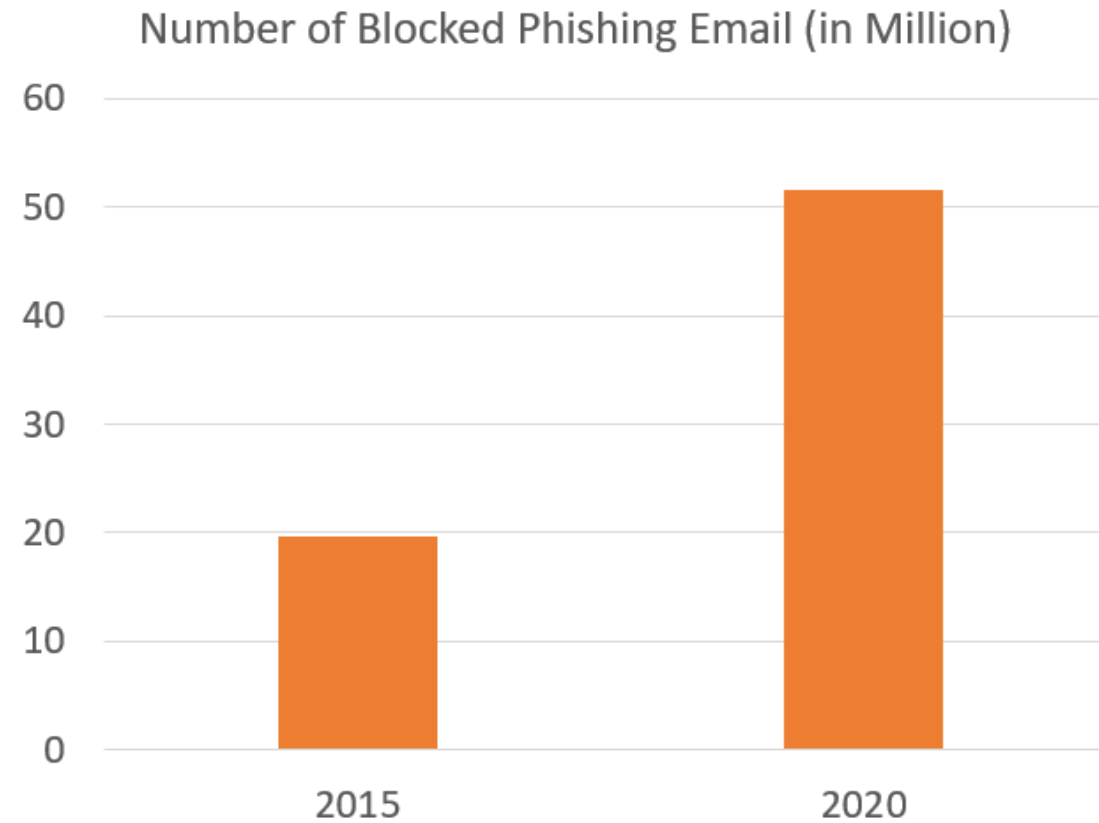


- ▶ Insufficient awareness training among healthcare workers
- ▶ High demands for anytime anywhere access

Phishing Attacks to End User - the Weakest Link

COVID-19 Themed Phishing Email Attack

- ▶ Scams (sell mask, vaccine, cures)
- ▶ Credential Theft
- ▶ Malware
- ▶ Ransomware



Source: HA Information Security Office

Ransomware is a key cyber threat for healthcare

- ▶ Increased ransomware attacks globally
- ▶ Clinical services were impacted seriously
- ▶ German reported the first patient death case due to ransomware attack in 2020
- ▶ US UHS lost USD\$67 million due to ransomware attack in 2020
- ▶ Ireland HSE hit with USD\$20 million ransomware demand in May 2021
- ▶ HA blocked several ransomware attack attempts

UPDATE: UHS Health System Confirms All US Sites Affected by Ransomware Attack



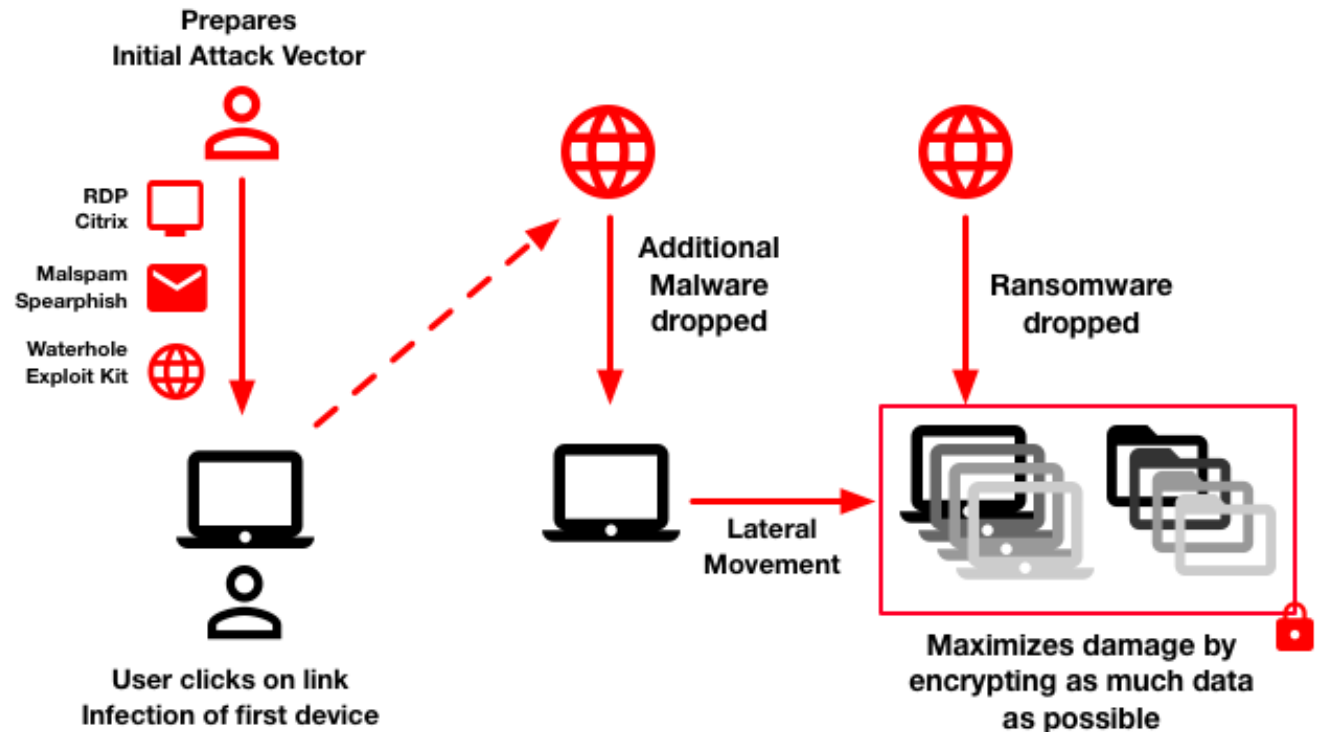
There is a significant ransomware attack on the HSE IT systems. We have taken the precaution of shutting down all our our IT systems in order to protect them from this attack and to allow us fully assess the situation with our own security partners.

2:28 PM · May 14, 2021

1.6K 191 Copy link to Tweet

The Ransomware behind the attacks – Conti

- ▶ Ransomware-as-a-service (RaaS)
- ▶ End-users are highly targeted
- ▶ Lateral movement for days
- ▶ Steal & encrypt data
- ▶ Double Extortion
- ▶ USD\$10-40 million ransom

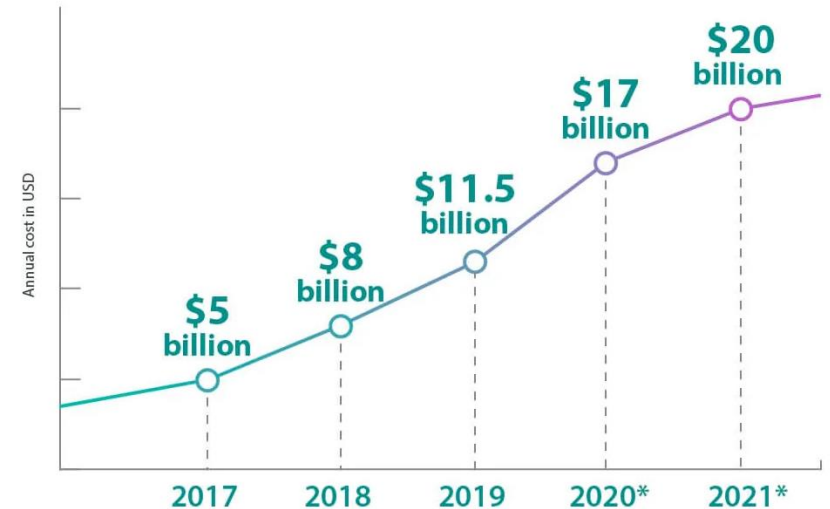


Ransomware would continue to hit the world

- ▶ Damage predicted to reach US\$20 billion by 2021

Defense Strategy

- ▶ Get the basic right (Hardening, Backup, etc)
- ▶ Assume the bad guys are already in
- ▶ Focus on detection and response capability
- ▶ Threat Intelligence from dark web
- ▶ Multiple layered approach - Defense in depth
- ▶ Cybersecurity & Cyber Resilience



Source: Cybersecurity Ventures



Source: peraton.com

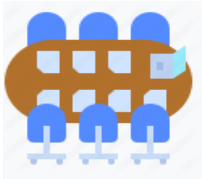


**KEEP
CALM
AND
BE
PREPARED**

Opportunity to improve Cybersecurity in Healthcare



Cybersecurity is treated as a patient safety issue



Cybersecurity risk is a board level agenda and priority



End users are more aware of cyber incidents and their impacts



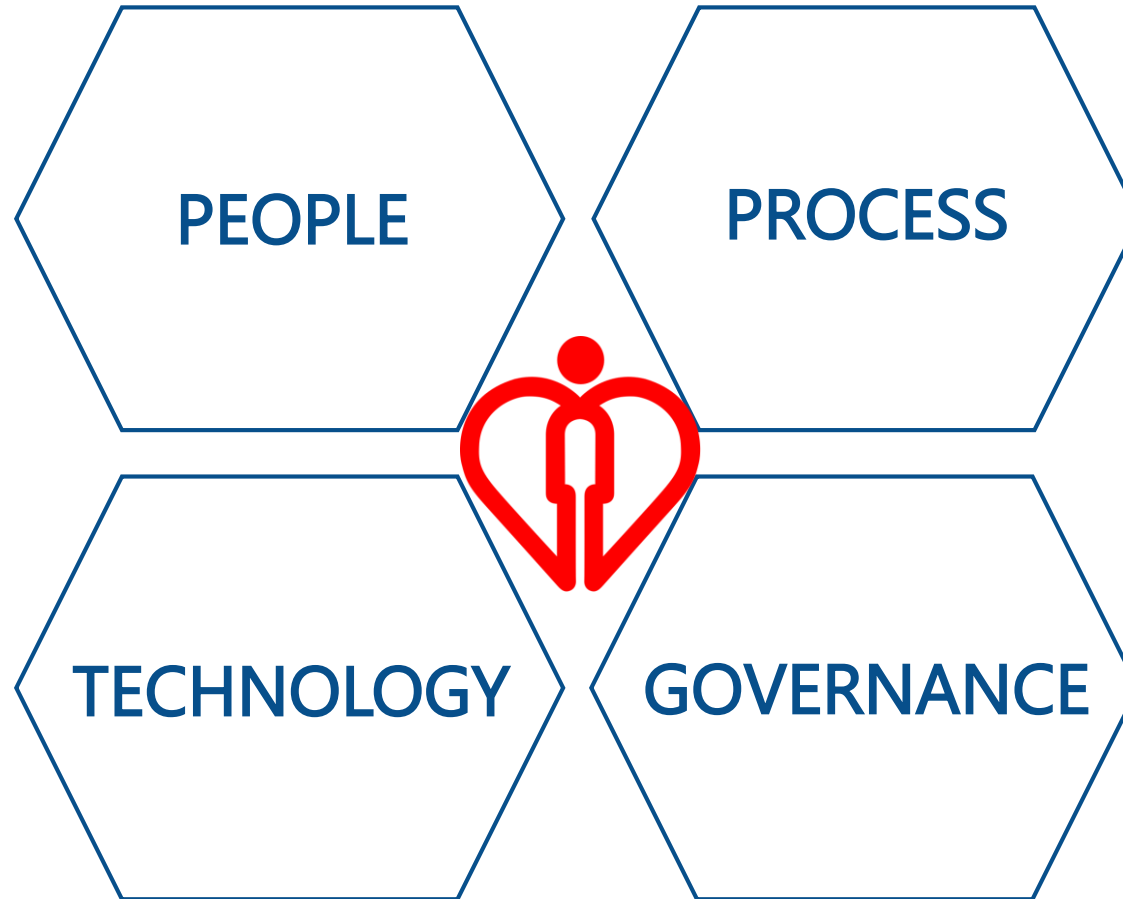
More security measures being developed for medical devices



Increased local and global cyber intel sharing network platforms

Start with a sound and practical Cybersecurity Strategy

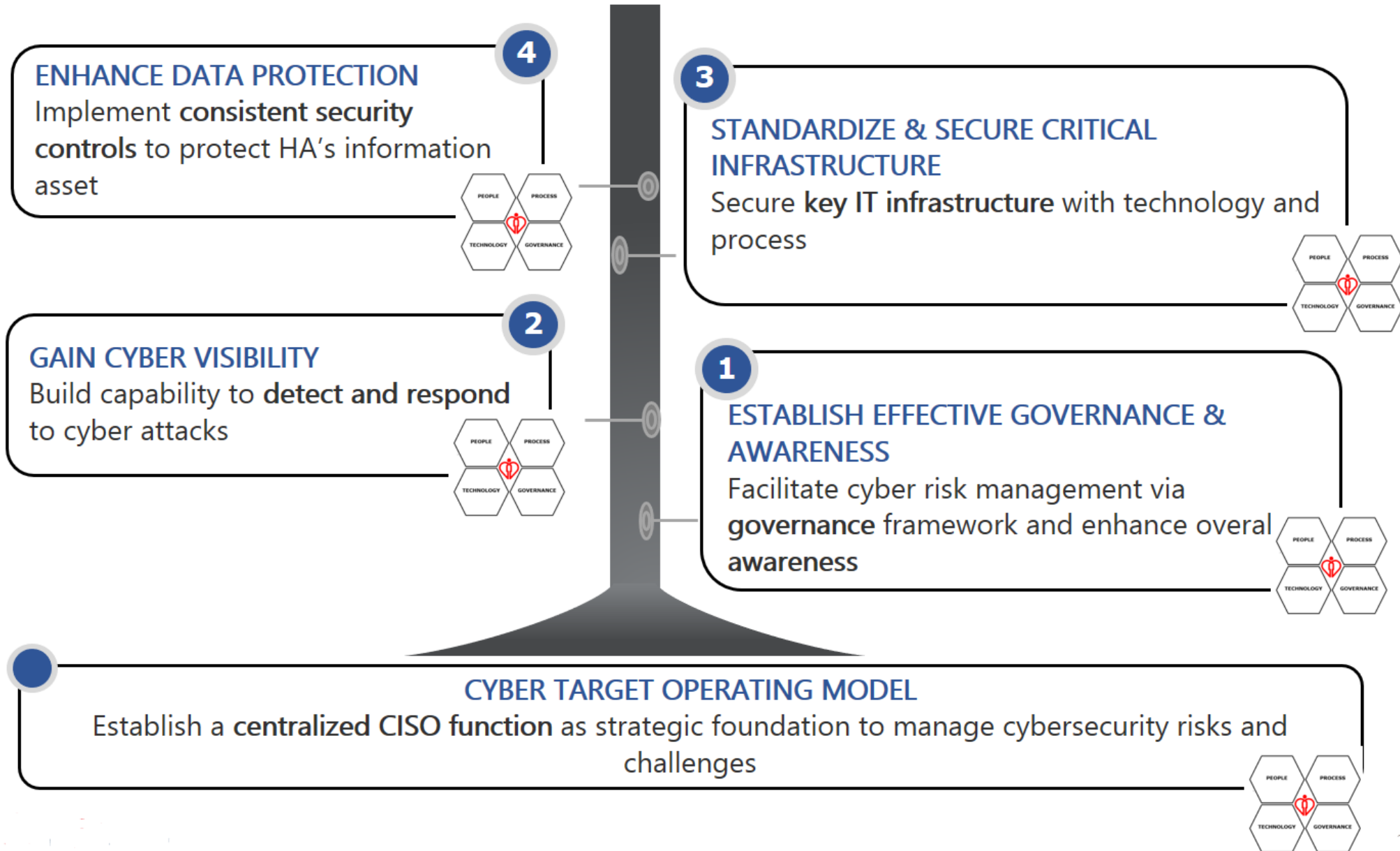
- Culture
- Awareness
- All Staff Engaged



- Prevention
- Detection
- Response

- Centralized
- Standardized
- Closed Loop
- Dedicated Function
- Targeted Ops Model
- External Collaboration

Start with a sound and practical Cybersecurity Strategy



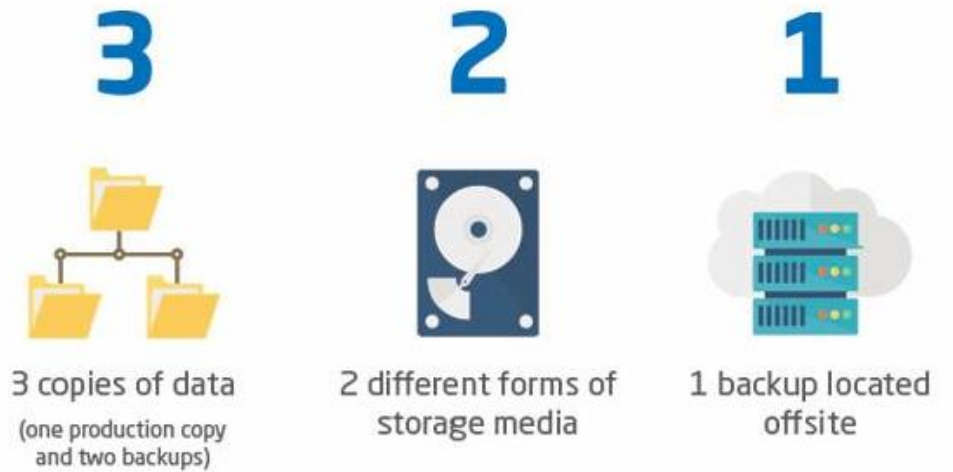
Get the basic right to avoid being low hanging fruit

<h2>備份和更新</h2>  <p>定期備份資料及 不要將備份連接至網絡</p> <p>為電腦系統和所有軟件 安裝最新的修補程式</p>	<h2>安全意識</h2>  <p>不要打開可疑的電郵， 及當中的附件和超連結</p> <p>不要瀏覽可疑網站，亦不要 從可疑網站下載任何檔案</p>
<h2>網絡和端點的保護</h2>  <p>安裝抗惡意程式碼軟件並保持 軟件與其識別碼為最新版本</p> <p>安裝網絡防火牆及 垃圾郵件過濾器</p> <p>定期全面掃描電腦</p>	<h2>安全設定</h2>  <p>停止或限制使用所有不必要的 系統服務或功能</p> <p>為所有系統及服務的設定採用 「最小權限」的原則</p> <p>關閉辦公室軟件內的巨集功能</p>

Source: HKCert.org

Plan and prepare for the worst

- ▶ Implement 3-2-1 Backup
- ▶ Establish a Business Continuity Plan (BCP)
- ▶ Drill the BCP plan regularly
- ▶ Engage business and users (e.g. PR)



Cultivate a cyber risk aware culture focusing on cyber hygiene

課程導航 Course Navigator

顯示/隱藏目錄 Show/Hide menu bar
課程進度 Tracking bar for overview

顯示/隱藏字幕 Show/Hide Captions

跳到指定章節 Navigate to specific topic

Real life cyber attack in Healthcare Industry

Real life examples on cyber attack in Healthcare Industry

To navigate this course, press the next slide button at the bottom right corner.

1 Best Practices for Meetings

- | | Host | Participant |
|----------------|------------------------------------------|--------------------------------------------------|
| Security level | 1 Use the latest version of Zoom client | 1 Use the latest version of Zoom client |
| | 2 Sign in with HA Internet Email | 2 [English] [中文] |
| | 3 DO NOT reuse meeting ID | 3 請回顧下面一封釣魚電郵的例子，及時刻謹記： |
| | 4 Set meeting password | 4 點擊連結前要先三思 |
| | 5 Check participants' Display Name | 5 有懷疑時不要提供任何個人資料 |
| | 6 Verify participant identity by video | 6 點擊Outlook 內的“Report Phishing Email”按鈕來報告任何可疑電郵 |
| | 7 Disable JOIN BEFORE HOST | |
| | 8 LOCK the meeting when meeting started | |
| | 9 Enable WAITING ROOM | |
| | 10 Set ONLY AUTHENTICATED USERS CAN JOIN | |

請回顧下面一封釣魚電郵的例子，及時刻謹記：

- 點擊連結前要先三思
- 有懷疑時不要提供任何個人資料
- 點擊Outlook 內的“Report Phishing Email”按鈕來報告任何可疑電郵

Cultivate a cyber risk aware culture focusing on cyber hygiene

提防網絡釣魚 報告可疑電郵

Be aware of phishing scams, report suspicious e-mails

網絡釣魚會利用我們心理弱點
Phishing e-mails take advantage of human psychological weaknesses

在 Outlook 點擊左邊紅魚圖標後可疑的釣魚電郵
Report phishing e-mails on Outlook by clicking the icon




- 1 核實寄件者**
Check the e-mail sender
(HA e-mail domain: @ha.org.hk)
- 2 向相關人士或部門確認**
Verify with the relevant persons or department
- 3 切勿回覆任何內部或個人資料**
Do not reply with any sensitive information or any personally identifiable information
- 4 切勿下載附件或點擊連結**
Do not download attachments or click links within the e-mail



強化密碼 保護大家

Strengthen passwords, start with you!



- 1 混合大小寫英文字母**
Include both uppercase and lowercase letters
- 2 包含數字或符號**
Include numbers or symbols
- 3 至少 8 個字元**
At least 8 characters
- 4 個人化密碼**
A complex but easily-remembered personalised password
(e.g. Red2011Paris!)
 - 最愛顏色 Favourite colour
 - 畢業年份 Graduation year
 - 印象深刻的城市 Memorable trip destination



連接安全網絡 避免不明Wi-Fi

Secure Wi-Fi connection, avoid unsecured free Wi-Fi

- 避免連接不明 Wi-Fi**
Avoid connecting to unknown free Wi-Fi
- 留意「安全」標示**
Pay attention to the "Secured" sign
- 使用 HA Wi-Fi**
Use HA Wi-Fi
 - HA-WPA2
 - HA-CORP-MOBILE
 - HA-MOBILE




Cultivate a cyber risk aware culture focusing on cyber hygiene

保護你的數碼身分小貼士



使用雙重或多重認證,以加強帳戶保安。



為不同的網上服務設定不同及高強度的密碼。



透露個人或敏感資料前再三思,提防釣魚網站攻擊。



如使用非個人電子裝置登入,切勿允許瀏覽器記住你的密碼。無需使用網上服務時,緊記即時登出帳戶。



刪除不再使用的帳戶,避免因忘記管理,未能及時察覺帳戶遭到入侵。



經常留意由服務供應商發出有關可疑帳戶活動或交易的通知,如有懷疑,應立即向服務供應商尋求協助。

Cybersecurity is a Team Sport

Everyone has a role to play



Thank you!

