

How to Protect Your Enterprise from Cyber Threats

Cybersecurity Manager
Arktos Lam

What if we don't care?

- Sensitive data breaches
- Lose customers confidence
- Profit loss & fines



Phishing Emails are also *evolving*

- Over 30,000 abusive commercial email attacks on businesses and services within 2 months
- HKCERT recorded over 10,000 cases of phishing websites within 4th quarter (2022)
- **Beware of Phishing Scams 3.0**

網絡安全2023 | 電郵攻擊變種! 2個月內發現33,817宗! 駭客隨時進入你的郵箱 | 4招防禦免中伏

2023.04.10 by 香港財經時報



網絡安全2023 | Check Point近日發現商業電郵攻擊變異提醒提防「網絡釣魚詐騙3.0」。單2個月內便有逾3萬宗濫用企業和服務發動電郵攻擊! 即睇4招防範!

Data Breaches: Top Reasons

- Outdated security softwares
- Malware
- Physical theft

...

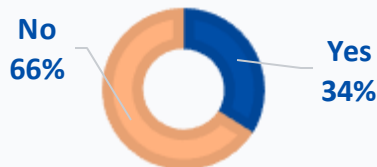
- **Human error/**
- **social engineering**



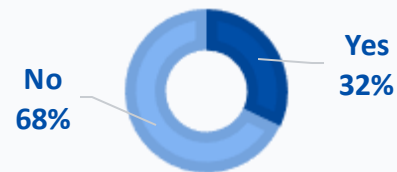
Survey on Staff Cybersecurity Training in Hong Kong

Size: 1-10
Micro-Businesses

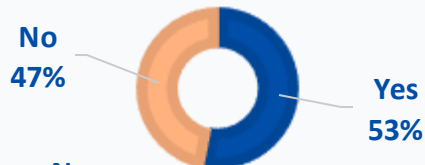
Has IT department/ Full-time IT staff



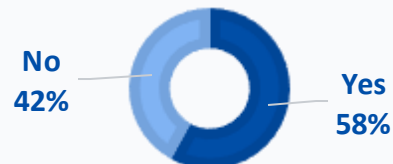
Employer Arranged Cyber Security Training During Onboarding



Size: 11-50
Medium-Businesses



Size: >50
Large Enterprises



About 240k companies & 1.4M workforce
lack cybersecurity training

Common Cybersec Risks in Work

- Passwords written on memos/sticky notes
- Leaving device unattended without logging out
- Using public WiFi for handling confidential data



Cybersec Training Hub

Cybersec Training Hub

Current Situation



Cyber Security Awareness



In Danger ☹️

- Work based on experience
- Not beware of risks

With the Programme



Much safer 😊

- Understand industry standard (e.g. remote working practice)
- Beware of potential risks

- ✓ Finish in 20 minutes
- ✓ Cyber security topics related to real-life business environment
- ✓ Free and easy to use for SMEs



Main Features



**Free and
Professional
Online Self
Training**



**Suitable to All
Staff, Do Not
Require
Technical
Knowledge**

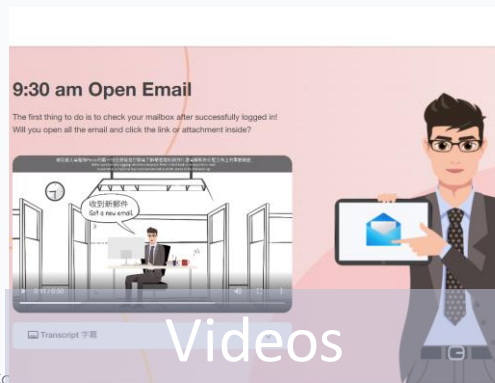
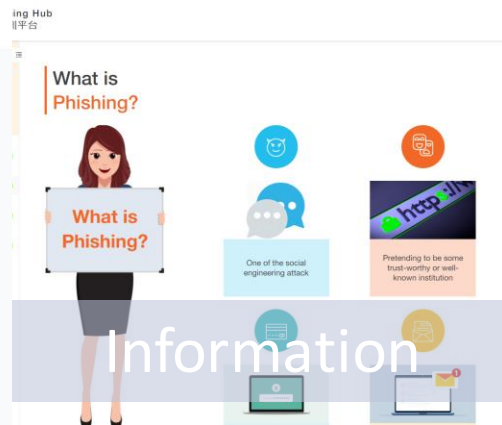
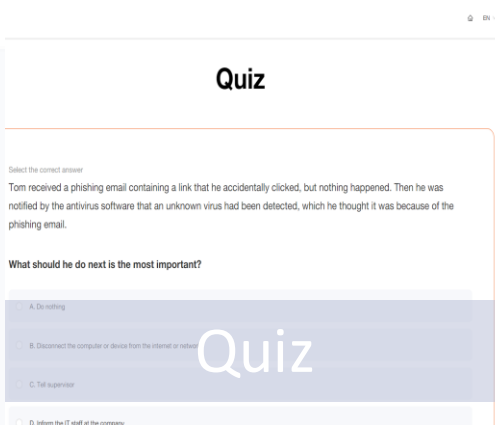


**Training
Contents
Simulate Real-
life Working
Environment**



**Easy for
Company to
Manage with the
E-Certificate
Issued after
Training**

Format



Suitable for different target groups



Phase 1
General Staff



Phase 2
Role-specific

- e.g.
- Human resource
 - Senior management
 - Finance & accounting
 - Marketing **(NEW!!)**



Phase 3
Sector-specific

- e.g.
- FSI
 - NGO
 - Retail

General Staff Training – From the perspective of Daily Work!



9:00 Get to Work and Log In - Password

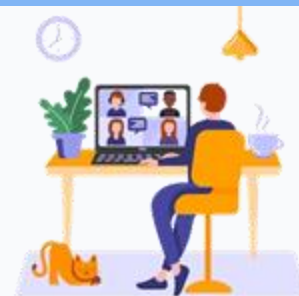


9:30 Open Email - Phishing

14:00 General Tips for Daily Operation



12:00 Lunch Time – Remote Working



Example on Role-specific (Human Resource Management)



- Handling the departure of staff

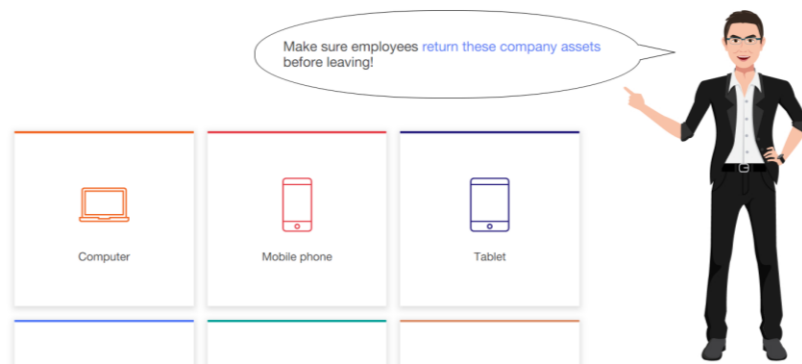
Access Rights on Company Accounts

Secure Handling of
Access Rights for Ex-Employees



Physical Assets Security

Physical Assets Security



Example on Role-specific (Senior Management)

- Protect the Company Band Image

Harmful to Company Brand Image

Cybersquatting

Register the company's Internet domain name first and then sell it to the company at a high price



A student in Hong Kong registered Hutchison Whampoa's Chinese domain name and sold it on his website for US\$1 million.

Social Media Impersonation

Fake social media accounts to impersonate real accounts to fool users



Cybercriminals posing as LinkedIn sent phishing emails to users to trick victims into logging in to a fake login page.

Email Spoofing

Send email using a fake sender address, such as impersonating business executive



Fraudsters hacked into the account of chief executive of multinational companies and asked staff to remit funds amounting to HK \$270 million to designated bank accounts on the grounds of urgency.

Fraudulent Website

Fake similar websites to mislead readers into believing they are official



[View example](#)

A fraudster posing as the MTR's website invited members of the public to participate in a customer satisfaction survey for a reward for five free one-way tickets.

Example on Role-specific (Finance & Accounting)

- Invoice fraud & other frauds targeting finance & accounting

Invoice Fraud (Vendor Impersonation)

Invoice Fraud



What is Invoice Fraud?



01

It's a form of social engineering attack



02

By impersonating the company's suppliers, business partners or executives



03

In order to deceive the employees to remit to the fraud account



04

Prevention of Business Email Compromise

How to Prevent Business Email Compromise

In 2020, the Hong Kong Police Force received 639 commercial email fraud cases with a total loss of more than \$2.2 billion, or an average loss of nearly 3.5 million per case, of which 70% of the victim companies were local SMEs

We must keep alert so that we will not fall into the trap of fraud easily!



01

Don't fall for sudden changes in remittance





Example on Role-specific (Marketing) **NEW!**



- Protecting CRM Data & protect against Negative SEO attacks

Protecting the CRM Data

Tips for protecting the CRM data

-  **01** Partner with a trusted CRM vendor
-  **02** Do not share the CRM account and password
-  **03** Monitor CRM system activity, e.g. unauthorized access, security breach alerts
-  **04** Execute the established backup plan every day to back up the CRM data



Protecting Against Negative Search Engine Optimization (SEO) Attacks

According to a research report published by HKIRC in 2022, 60% of the companies pay attention to SEO, but 75% have never heard of negative SEO attacks. Also, 72% of them know that Trojan horse programs and virus intrusions will lead to a drop in SEO rankings, but they are unfamiliar with other tactics of hackers! Enterprises should pay more attention to related risks!



Enable Email Notifications

Monitor the Social Media

Protect Website from Hackers & Malicious Emails

Protect against Website Content Thieves

Pay attention to information and issues related to the website organised by the website administrator, and be able to take immediate countermeasures

Avoid bad publicity by monitoring social media platforms

Enhance website security and increase employee security awareness to avoid hacking

Find the text content of highly overlapping website articles on the Internet





Cybersec Training Hub
網絡安全員工培訓平台

免費 | 專業 | 一站式平台

員工網絡安全培訓
必睇網站



cyberhub.hk



How do your organisation adopt the platform ?

What if I want to keep track of completion status?

Cybersec Training Hub

Step 1


- Create an online form that allows file upload
- Select the file upload as a required field
- Restrict to Only people in my organisation can respond



Cybersec Training Hub

Step 2


- Create a leaflet with QR code that leads to the form created
- Or an electronic copy in order to be more environment-friendly
- Hand out to new employees




Cybersec Training Hub

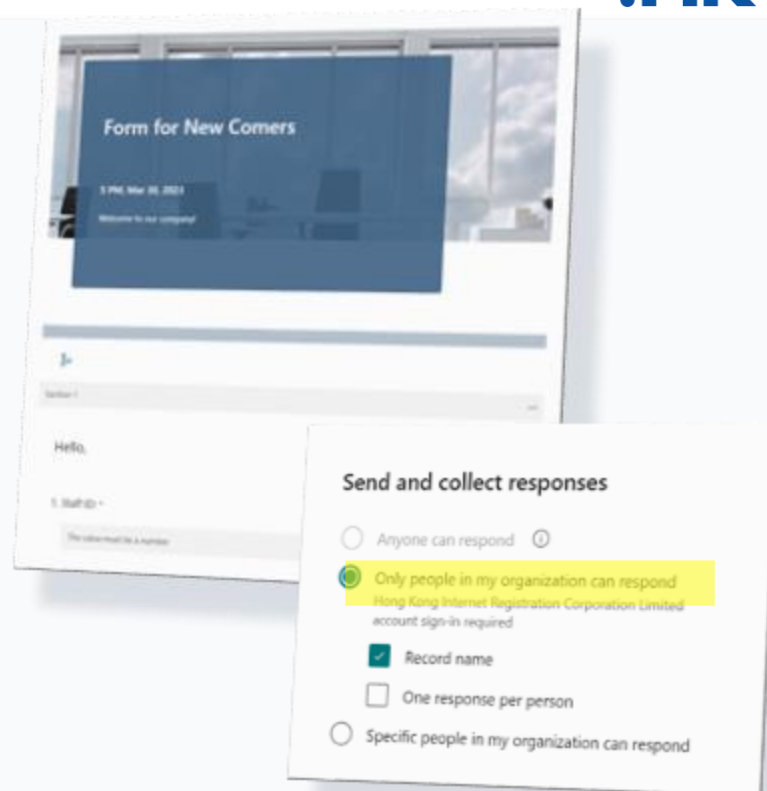
Step 3

- Leverage the online form platform's response management
- Check respondent's file upload of the cert. of completion



Step 1

- Create an online form that allows file upload 
- Select the file upload as a required field
- Restrict to Only people in my organisation can respond



Step 2



- Create a leaflet with QR code that leads to the form created
- Or an electronic copy in order to be more environment-friendly
- Hand out to new employees



Step 3

- Leverage the online form platforms' response management
- Check responders' file upload of the cert. of completion



Keep posted to cybersecurity trend via information sharing



Cybersec Infohub

- A partnership programme jointly administered by
 - Office of the Government Chief Information Officer (OGCIO) and
 - Hong Kong Internet Registration Corporation Limited (HKIRC)
- To promote closer collaboration **among local information security stakeholders of different sectors**
- Members can **share cyber security information under a secure platform to jointly defend against cyber attacks**



Major Internet
Service Providers



Critical Infrastructure
Operators



Finance & Insurance



Innovation &
Technology and
Information Security



Education

GovCERT.HK



Local Computer
Emergency Response
Team Coordination Center



Other Industries

Membership



- Any local organisation with its business address in Hong Kong and owns a “.hk” Internet domain name
- Manage an electronic communications network and have operational needs for cyber security information
- The membership is **free-of-charge**





Programme Benefits

By joining the Programme, organisations can enjoy a wide range of benefits including:

Join member-exclusive activities

e.g. seminars, technical workshops, industry-specific meetings, etc.

Enjoy collaborative and networking opportunities with cyber security experts

Receive early warnings of cyber threats and insights from experts of different sectors

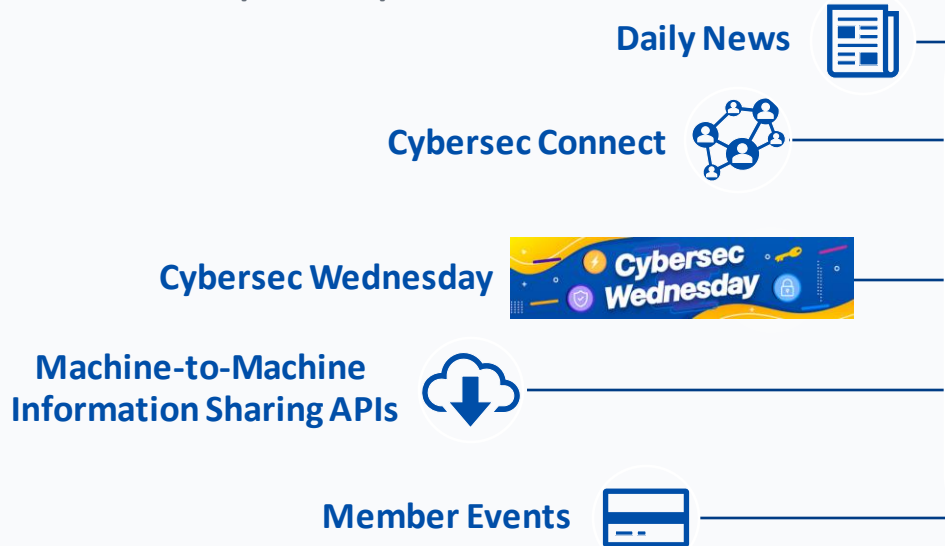
Ask cyber security questions or seek advice from industry experts on the platform

Anonymous posting option is available!



Highlights of Cybersec Infohub

- ✓ Cyber security information for both IT specialists and business users
- ✓ Various new features/services/events introduced:



Thanks

