

The First Line of Defence Against Cybersecurity Threats in Healthcare

Eric Cheng

Quality HealthCare Medical Services Limited

21-10-2024

Healthcare Sector

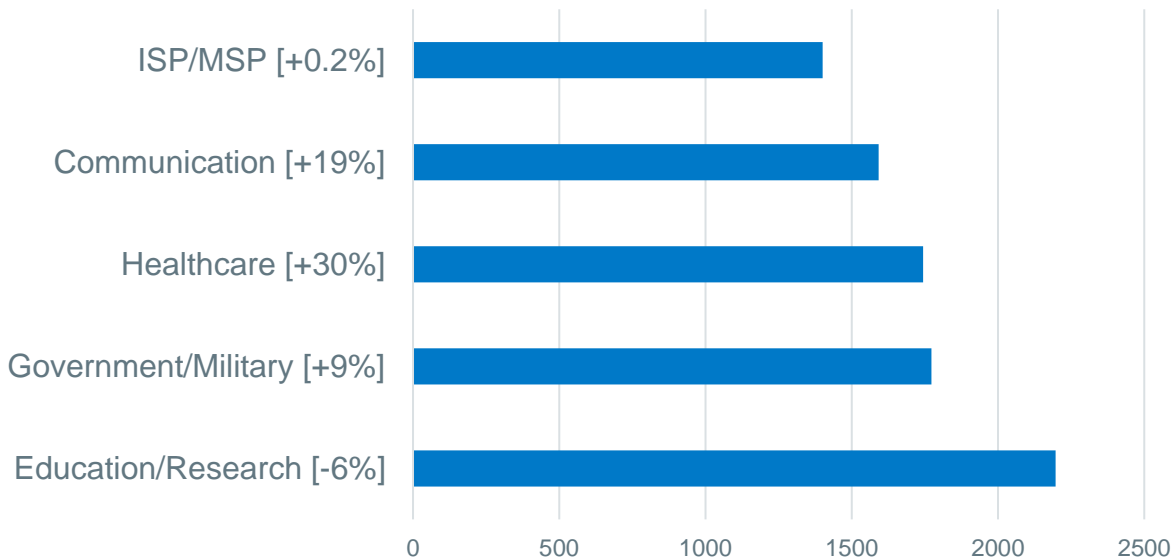
Prime target of Cyberattack

Statistics on Cyberattacks – Healthcare

Average Weekly Attacks

The **Healthcare** sector followed closely behind, with an average of **1744** attacks per week, reflecting a significant YoY increase of **30%**.

Average Weekly Attacks



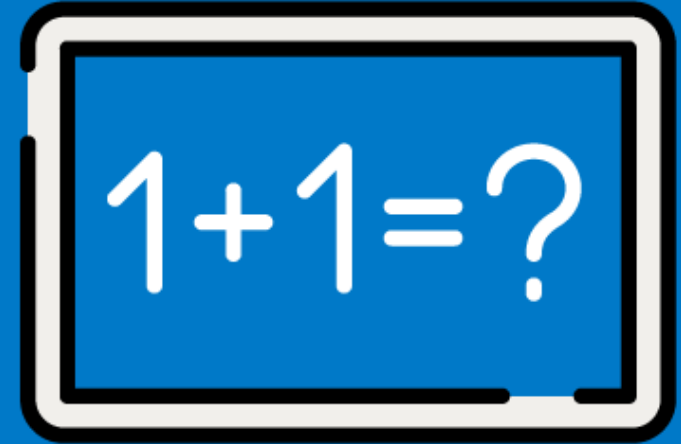
<https://blog.checkpoint.com/security/average-weekly-global-cyberattacks-peak-with-the-highest-number-in-2-years-marking-an-8-growth-year-over-year-according-to-check-point-research/>

Global Ransomware Attacks per Industry

Healthcare has a high attack ratio, with 1 out of 27 organizations attacked. The 16% increase in attacks year-over-year highlights growing risk.

Industry	Organization Attacked Ratio	YoY Change
Consultant	1 out of 38	128%
Insurance/Legal	1 out of 47	71%
Utilities	1 out of 37	60%
Transportation	1 out of 49	43%
Leisure/Hospitality	1 out of 55	41%
Finance/Banking	1 out of 31	33%
Communications	1 out of 37	24%
Healthcare	1 out of 27	16%
SI/VAR/Distributor	1 out of 41	15%
Software vendor	1 out of 65	13%
Hardware vendor	1 out of 73	7%
ISP/MSP	1 out of 36	2%
Education/Research	1 out of 31	-2%
Government/Military	1 out of 25	-4%
Retail/Wholesale	1 out of 60	-11%

Why Healthcare?



Why Healthcare?



Medical Data Is Valuable

- Healthcare organizations store valuable personal information, including medical histories, and insurance details, making them attractive to hackers.

The medical records of patients can sell for as much as **\$1,000 on the dark web.**

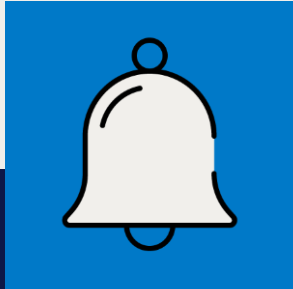


The black market value of medical records **stands at \$250 (on average).**



Medical records are valuable because **they contain lots of sensitive data**, which cannot be changed easily by victims.

Why Healthcare?



Paying the ransom

- Nearly half (47%) said their organizations experienced a ransomware attack in the past two years
- In a 2022 Sophos survey of healthcare IT professionals, a solid majority (61%) acknowledged that their organizations paid a ransom, well above the average of all industries (46%)

US\$197K

average ransom payment by healthcare, lowest across sectors



33%

increase in healthcare ransom payment over previous year



60%

ransom amounts in healthcare less than US\$50,000

Why Healthcare?



COVID-19 App

- COVID-19 apps were highly vulnerable due to rushed and subpar development
- Significant majority of these apps exhibited major security flaws,

High-Profile COVID-19 Data Leaks

Pfizer Breach

- Hackers breached the European Medicines Agency and stole data related to Pfizer's COVID-19 vaccine candidate

Wales Patient Data Breach

- Public Health Wales accidentally posted COVID-19 patient data for 18,000 residents on a public-facing database for 20 hours

Brazil COVID-19 Data Breach

- A Brazilian hospital employee inadvertently exposed sensitive data of 16 million COVID-19 patients, including the President of Brazil

Germany's COVID-19 Tracking App

- A remote code execution vulnerability was discovered and swiftly addressed in Germany's COVID-19 tracking app

Weakest Link in Cybersecurity

01

Technology

- It follows programmed **instructions** and provides **repeatable outputs**.
- Security vulnerabilities can exist, but these **can be fixed** with updates.

02

Process

- Processes are a series of steps designed for **consistent outcomes**.
- Broken processes can **be reviewed and fixed** with clear solutions.

03

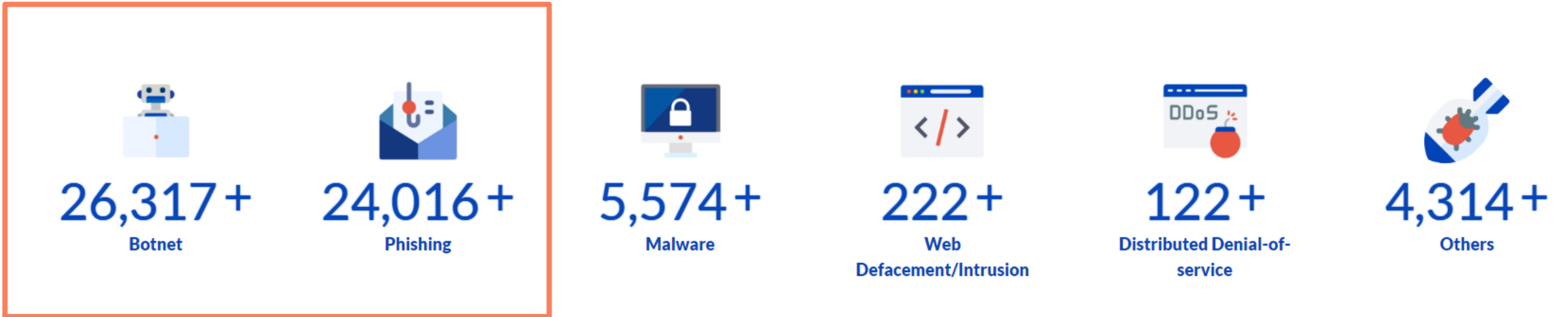
People

- People make independent decisions, sometimes irrationally and **unpredictability**.
- Errors are common and **unpredictable**, despite awareness training.

“Humans Are the Weakest Link in Cybersecurity”

Incidents in Hong Kong

Incidents reported to Hong Kong Computer Emergency Response Team Coordination Center(香港電腦保安事故協調中心) since 2018

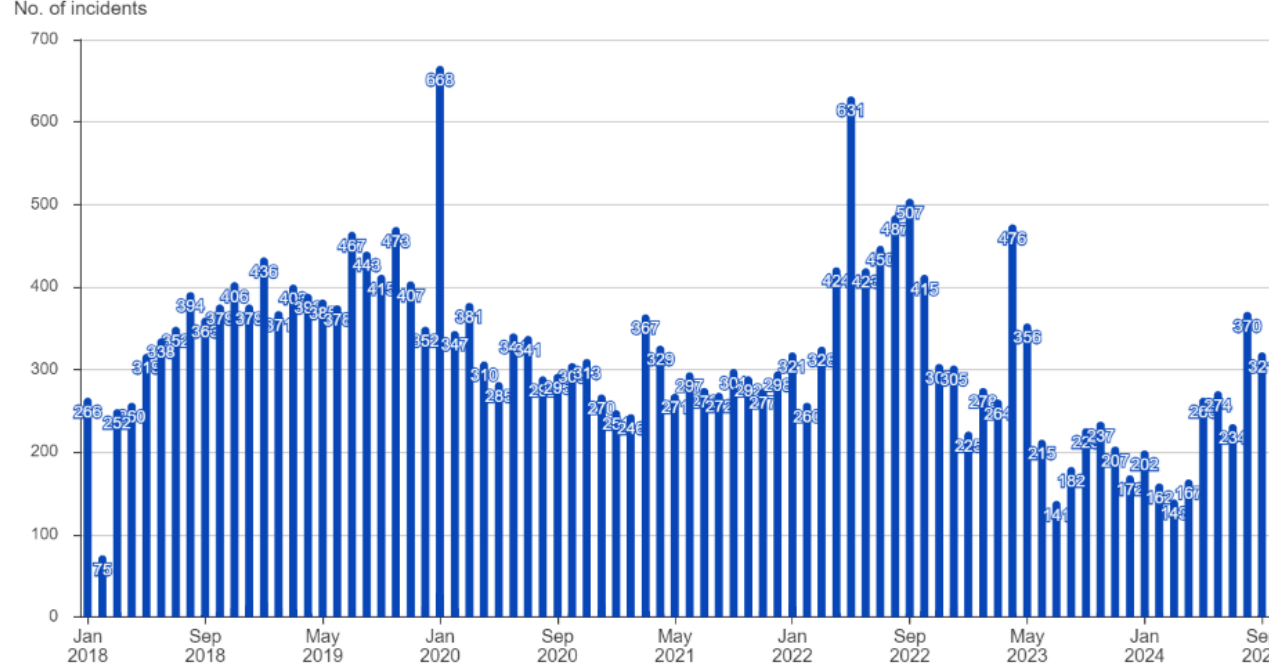
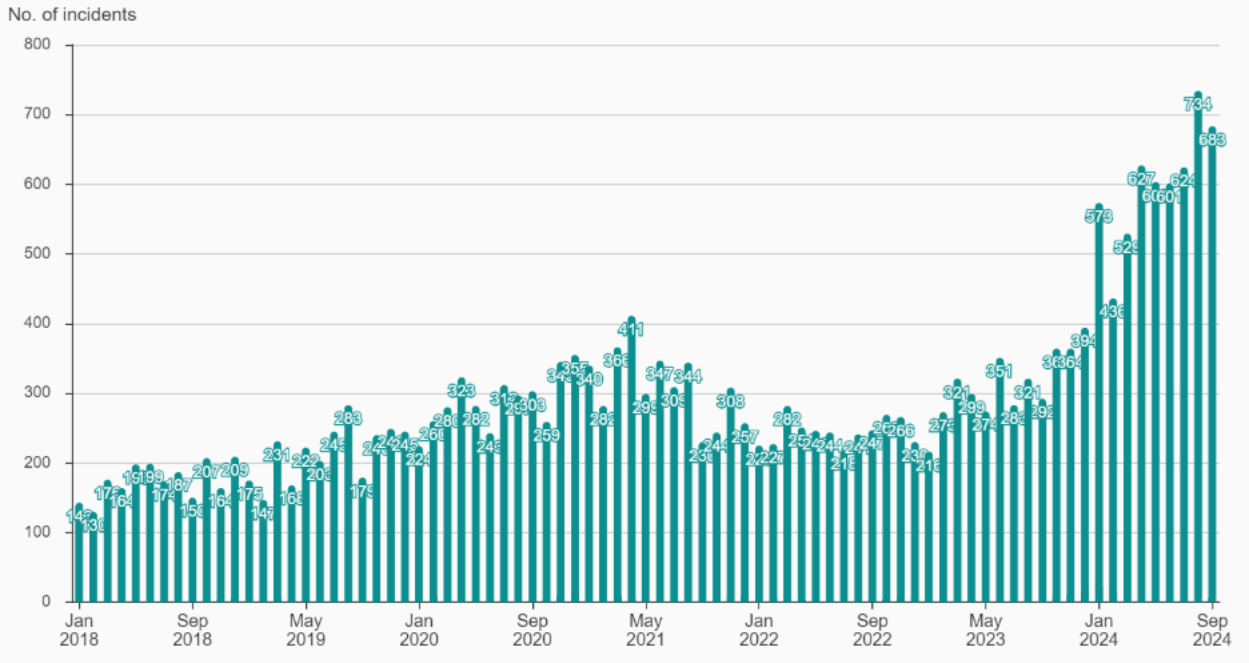


Botnet and **Phishing** are TOP 2 types of incident

Incidents in Hong Kong

Phishing

Botnet

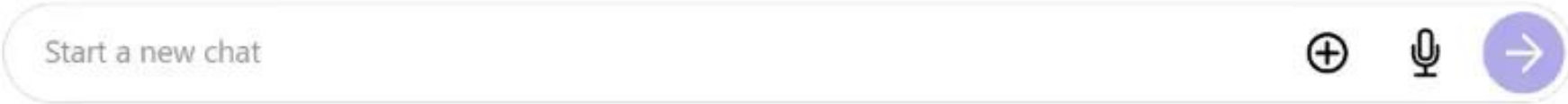


Significant increase of Phishing incident since 2023

Steady / drop of Botnet since 2023

Live Demo

Took AI less than 5s to draft legitimate phishing email 🙄



Cyberattack Prevention

1

**Proper
Device
Security**



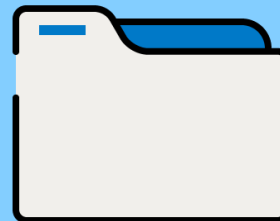
2

**Identify
Risks
Entry**



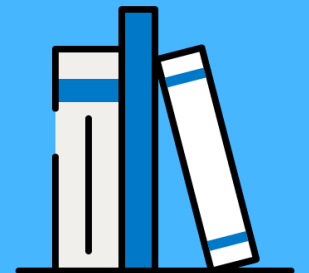
3

**Backup
&
Update**

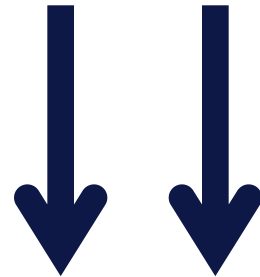


4

**Education
Is
Key**



**“ Humans are the
weakness link. “**



**People are our first
line of defence.**



How Can We Equip the People?



Training + Awareness Program



Training

- Provide regular training
- Provide Up-to-date material
- Apply to their real lives
- Offer hands-on capabilities

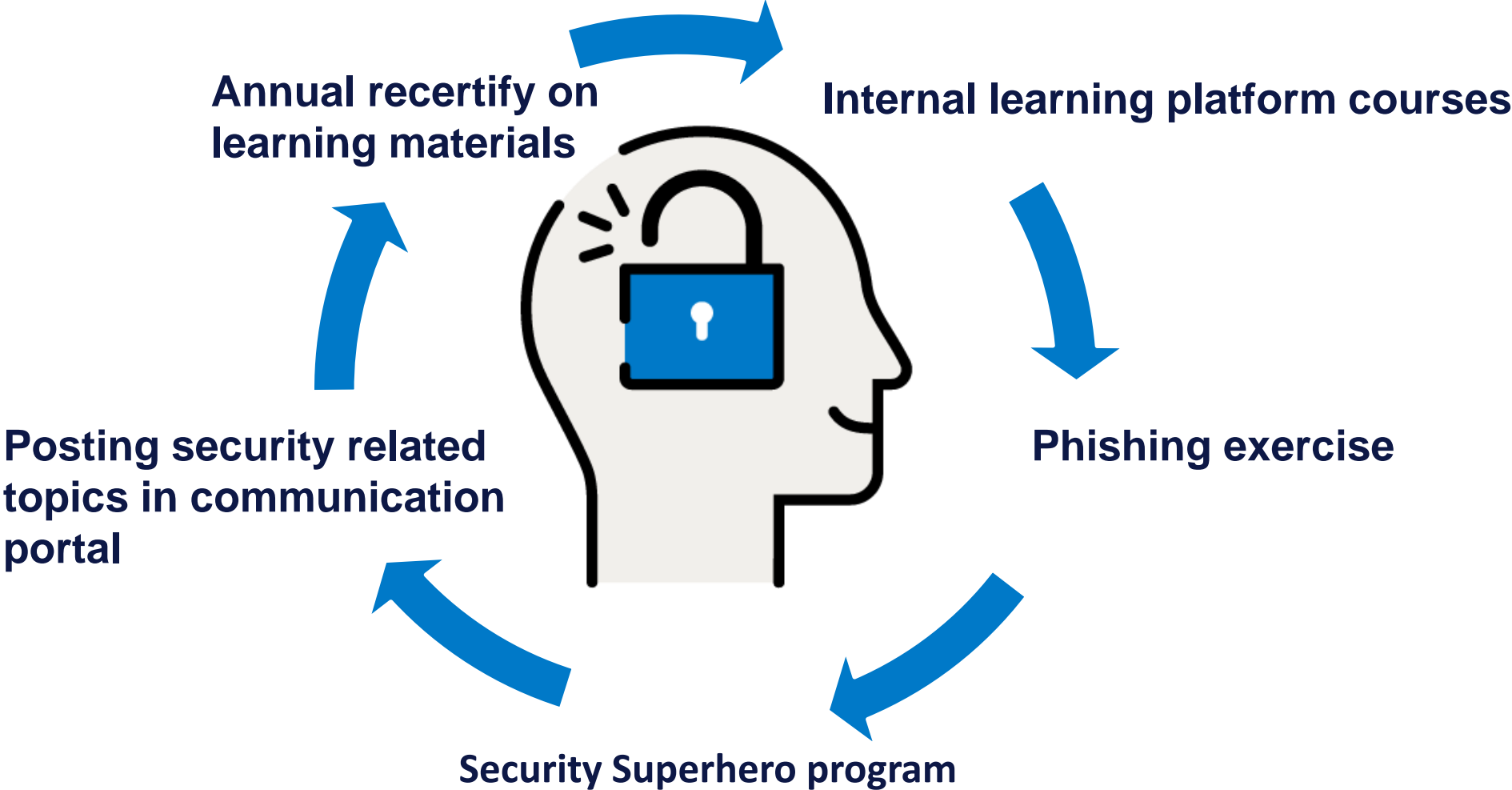


Awareness Program

- Educate employees on recognizing phishing and social engineering attacks.
- Promote a security-first mindset across the organization.



Training + Awareness Program



Annual recertify



My Courses and Learning Plans

All the courses and learning plans in which you're enrolled, including all of your courses in progress and already completed.

FILTERS

information



NEWEST TO OLDEST (ENROLMENT) ▾

5 Items



In progress

Keeping Information Safe
Expiration: 10/9/2024

EN | 20m 00s

E-learning



Completed

Personal Data Retention

EN | 15m 00s

E-learning



Completed

Information Matters (HKHI)

EN | 15m 00s

E-learning



Completed

Information Security
Awareness for Privileged
Users

EN | 15m 00s

E-learning



Completed

Payment Card Industry DSS
Awareness (HK)

EN | 20m 00s

★ 5.0

E-learning

Conduct simulation exercise regularly with different themes

Impersonating

2. Sender's email address appear suspicious or unfamiliar?

1. Treat all emails from outside of Bupa with extra care

A document requires your signature <documents@docsign-online.net>

AD To LEUNG, Joyce

Retention Policy 7 Year Delete (7 years)

Expires 8/20/2031

Wed 8/21/2024 11:53 AM

Please be aware. This email originated from outside of Bupa. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Adobe Sign

Hi joyce.leung@bupa.com.hk
Fiona Harris requests your signature on a document.

<https://login.yggui.li/bupa/f2d287031433a6a8?l=58>
Click or tap to follow link.

Review and sign


3. Hover over URLs to check the destination before clicking.

Dear all,

Please review and sign the attached document at your earliest convenience.

Thank you,

FIONA HARRIS - MANAGING DIRECTOR
fiona.harris@bupa.com.hk



Report Phish
PhishAlarm



Fail ???

1. Treat all emails from outside of Bupa with extra care



Breakfast is on us!

In partnership with your organization we are giving away 10,000 free breakfast items in our establishments anywhere in the world. Scan this QR code to redeem your coupon.



Quishing

Provide focus training & mandatory assessment



Phishing Awareness In-depth Training

(By InfoSec)

Assessment – for course completion



IMPORTANT

- For course completion, please submit your answers (Q1 – Q10) through the [online assessment](#) within 3 days after the training
- 100% passing score is required for training completion
- If you got score below 100%, **re-do** the assessment is required

Passing
Score
100 %



**Redo
Assessment**



Importance of Reporting Phishing

01

Prevent future exposure

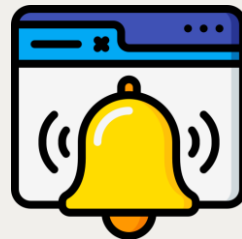
through the one-click action



02

Avoid incidents

notify other colleagues of the threat (if it's a real attack)



03

Show your security awareness

no two attacks are the same



Clear Policies and Guidelines

- **Establish and communicate clear cybersecurity policies**
- **Ensure easy access to these guidelines for all employees**



How it helps our People

- **Awareness:**

People will be aware of best practices for protecting their information, such as using strong passwords or recognizing suspicious emails. This lack of knowledge can result in unintentional security breaches.

- **Emotional and Psychological Stress:**

Experiencing a cyberattack or data breach can lead to significant stress and anxiety for individuals. The fear of identity theft or financial loss can have lasting emotional effects.

A clear policy can help people on handling the cyberattack



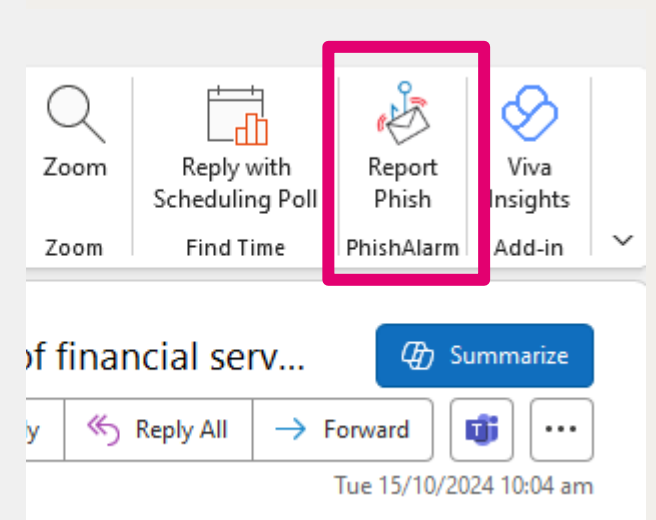
Encourage a Culture of Reporting

- Create a non-punitive environment for reporting suspicious activities
- Reward proactive behavior in identifying potential threats



How it helps our People

- Increase Trust
- Enhance Collaboration
- Detection Threats in Early Stage



Provide Tools and Resource

Provide the right tools - Don't overlook the critical need to enhance cybersecurity awareness training with practical tools



IDS / IPS Tools Penetration Testing

Data Loss Prevention

Email Security Tools Endpoint Detection

Privileged Access Management

Vulnerability Assessment

Network Detection Tools

Security information and event management

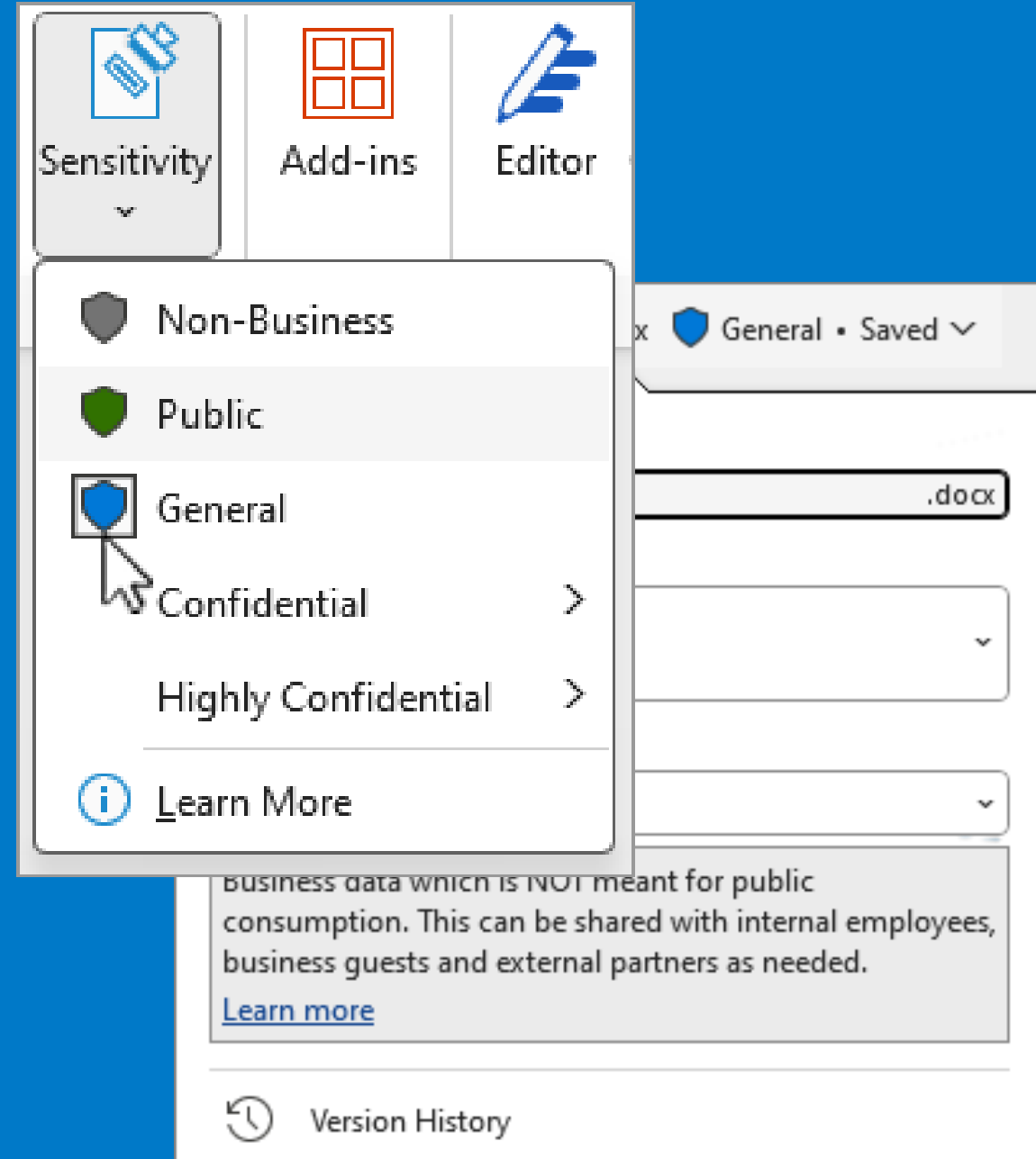
Sensitivity Label

Documents/Emails can be applied the “sensitivity label” to classify the data sensitivity level.

- **Public – Public Disclosure**
- **General – Business related and widely shared within organization**
- **Confidential – Data required protection (e.g. Medical History)**

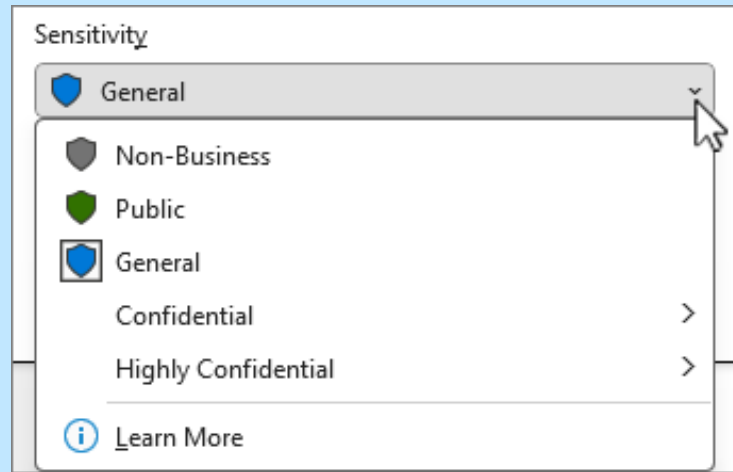
All saved documents and emails **MUST** be defined with sensitivity label.

Policies can be applied to restrict the sharing on documents / emails.

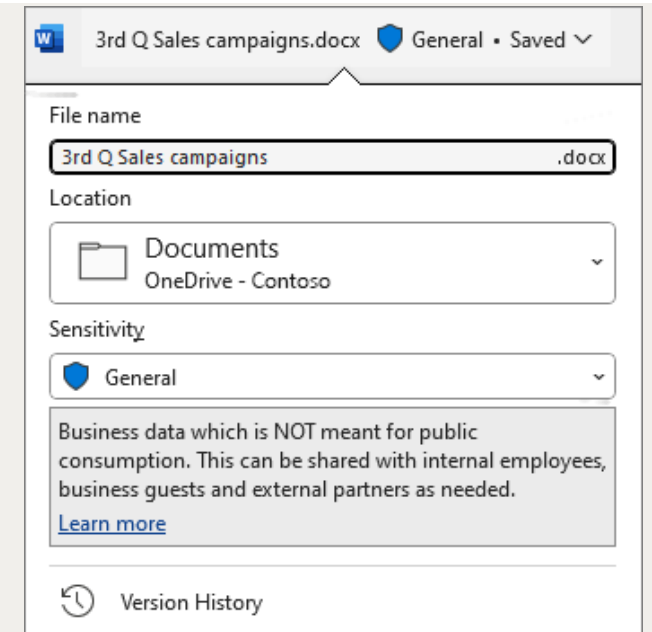


Sensitivity Label

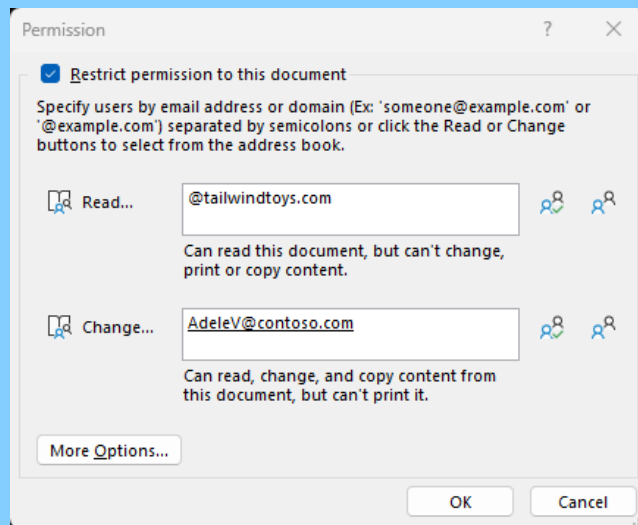
1. Define Sensitivity Labels:



2. Apply Labels to Documents



3. Set Up Policies



4. Educate



DLP Tools

DLP or Data Loss Prevention is a cybersecurity solution that detects and prevents data breaches.

It can be applied to various platforms and applications, including:

- Web Browser
- Email Client
- Endpoint Device
- File Sharing Service

Comparison

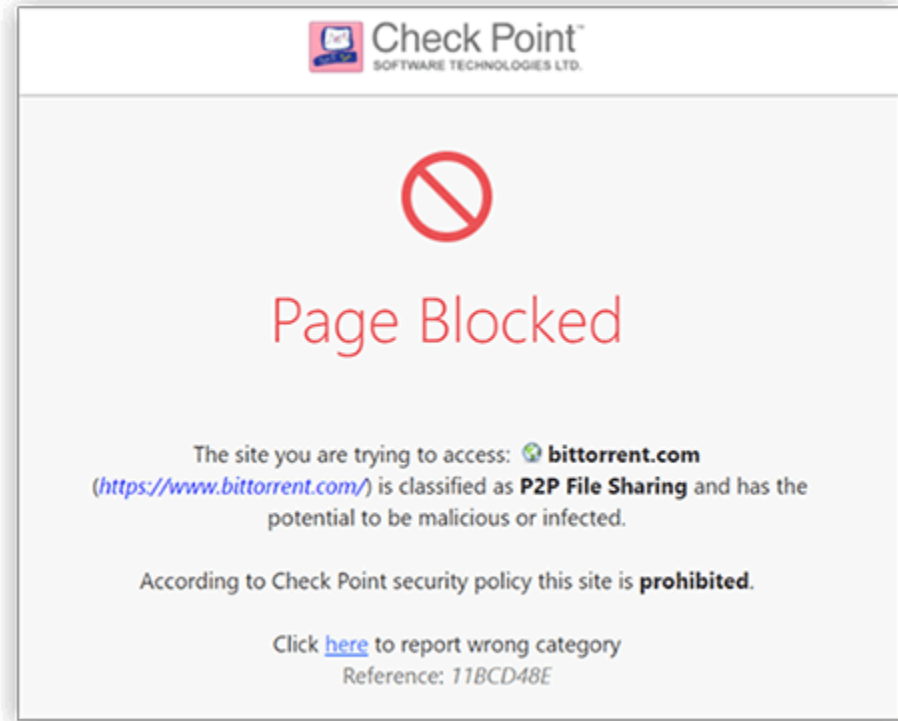
Firewall Network Protection

- It won't stop you from sending an email to your client.
- It focuses on keeping harmful traffic out of your network.

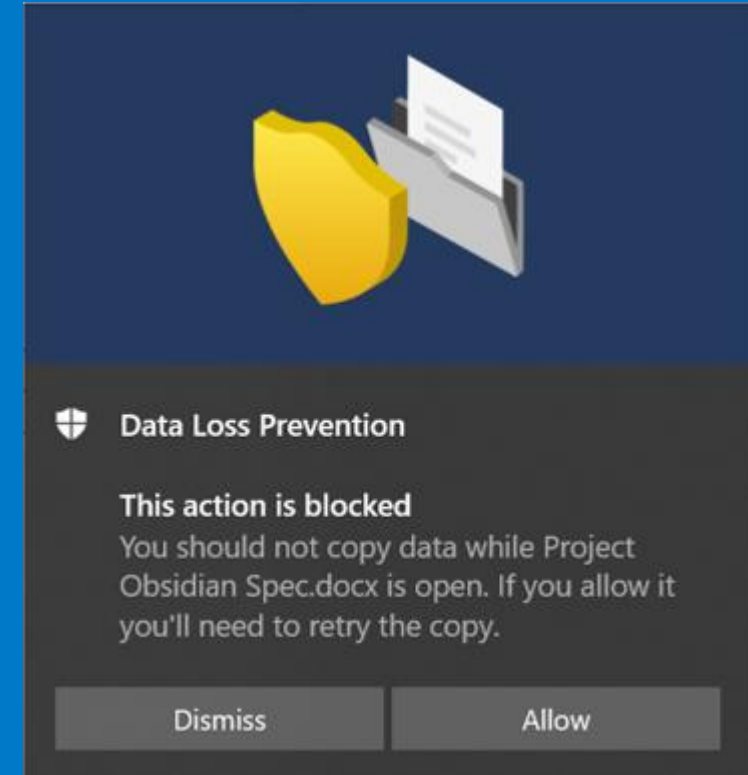
DLP Data Protection

- It will stop you from sending sensitive information, like confidential documents, to your client if it's not allowed.
- DLP ensures important data stays secure.

DLP Tools - Web Browser

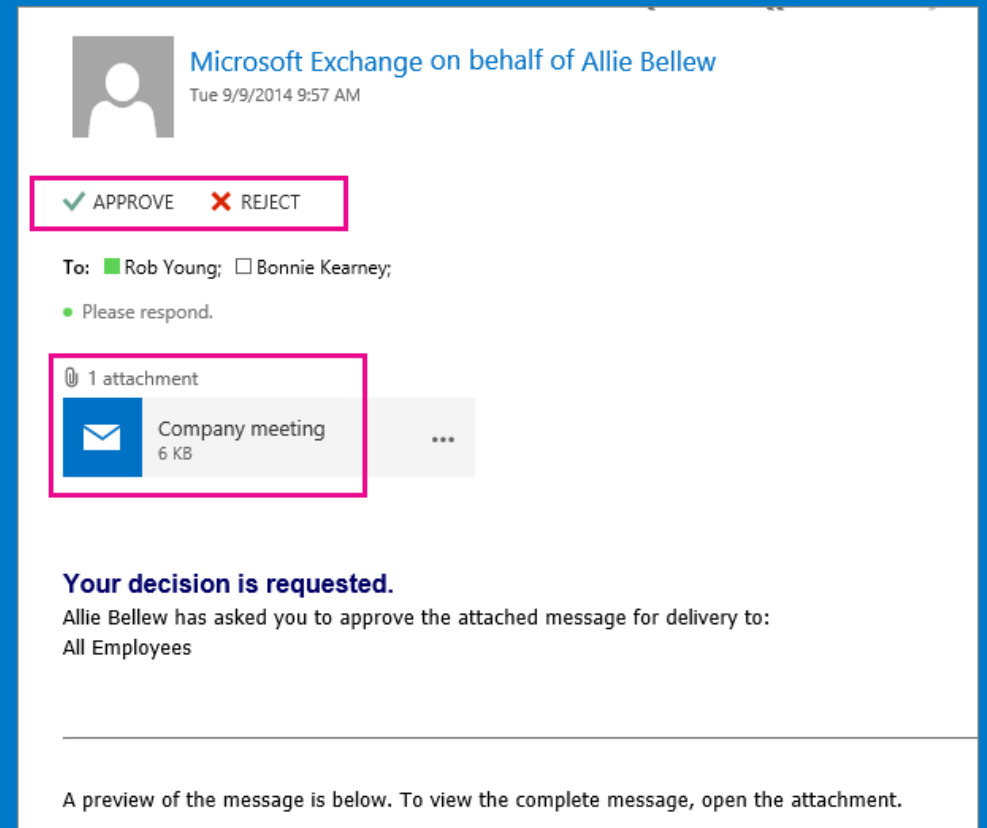
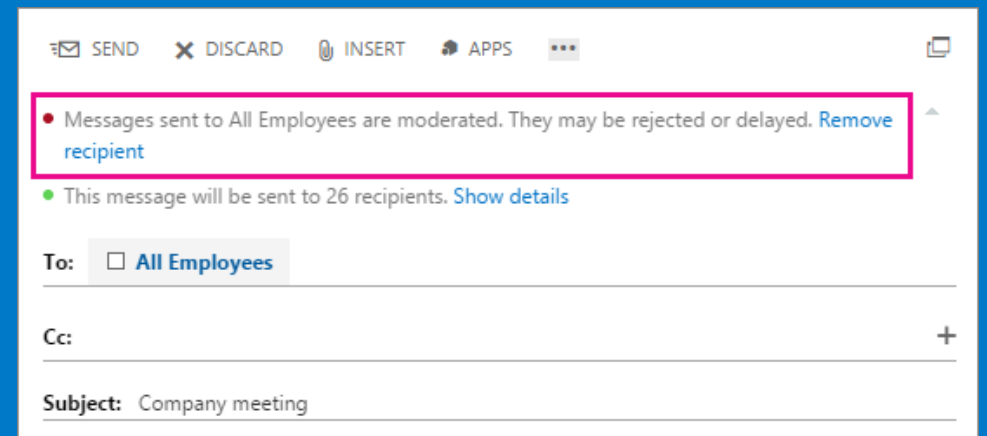
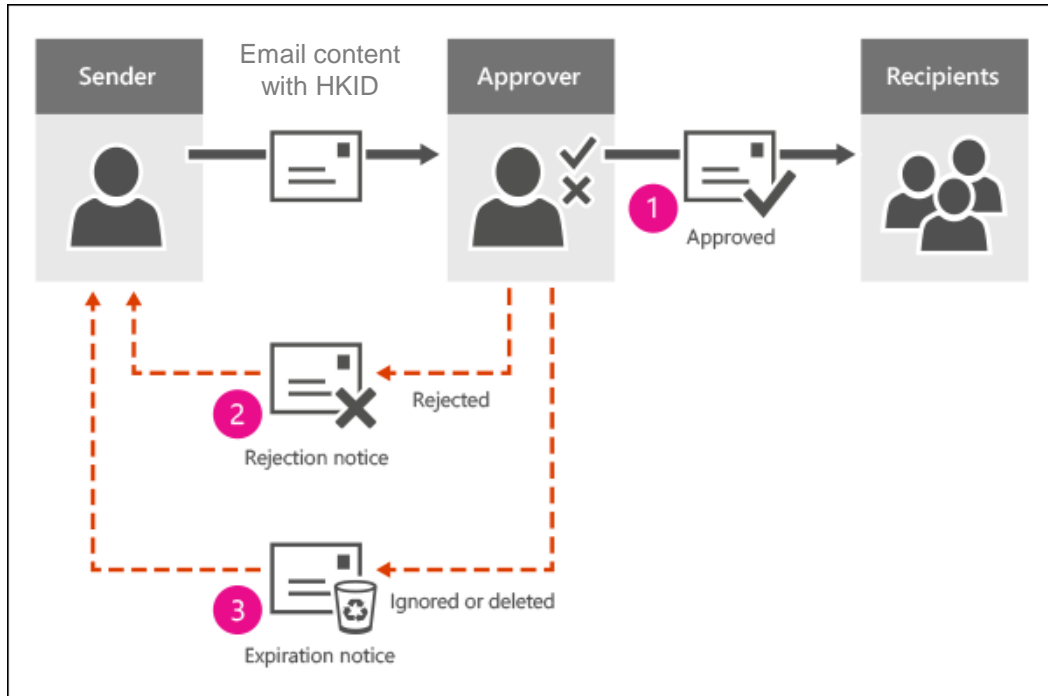


DLP Tools - File Sharing

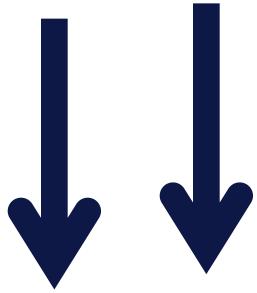


DLP Tools – Email Client

By integrating the DLP policies and email server moderated setting, emails with sensitive information **MUST** be required manager approval before sending out.



**People are our first
line of defence.**



**People are our
BEST line of
defence.**



**EVERYONE
MATTERS !**

Thank you

Eric Cheng

Quality HealthCare Medical Services Limited

21-10-2024