Data Privacy in 2021 - Things you need to know

The University of Hong Kong

03 November 2021

EY 安永

Building a better working world

Agenda

1 Basics of Personal Data

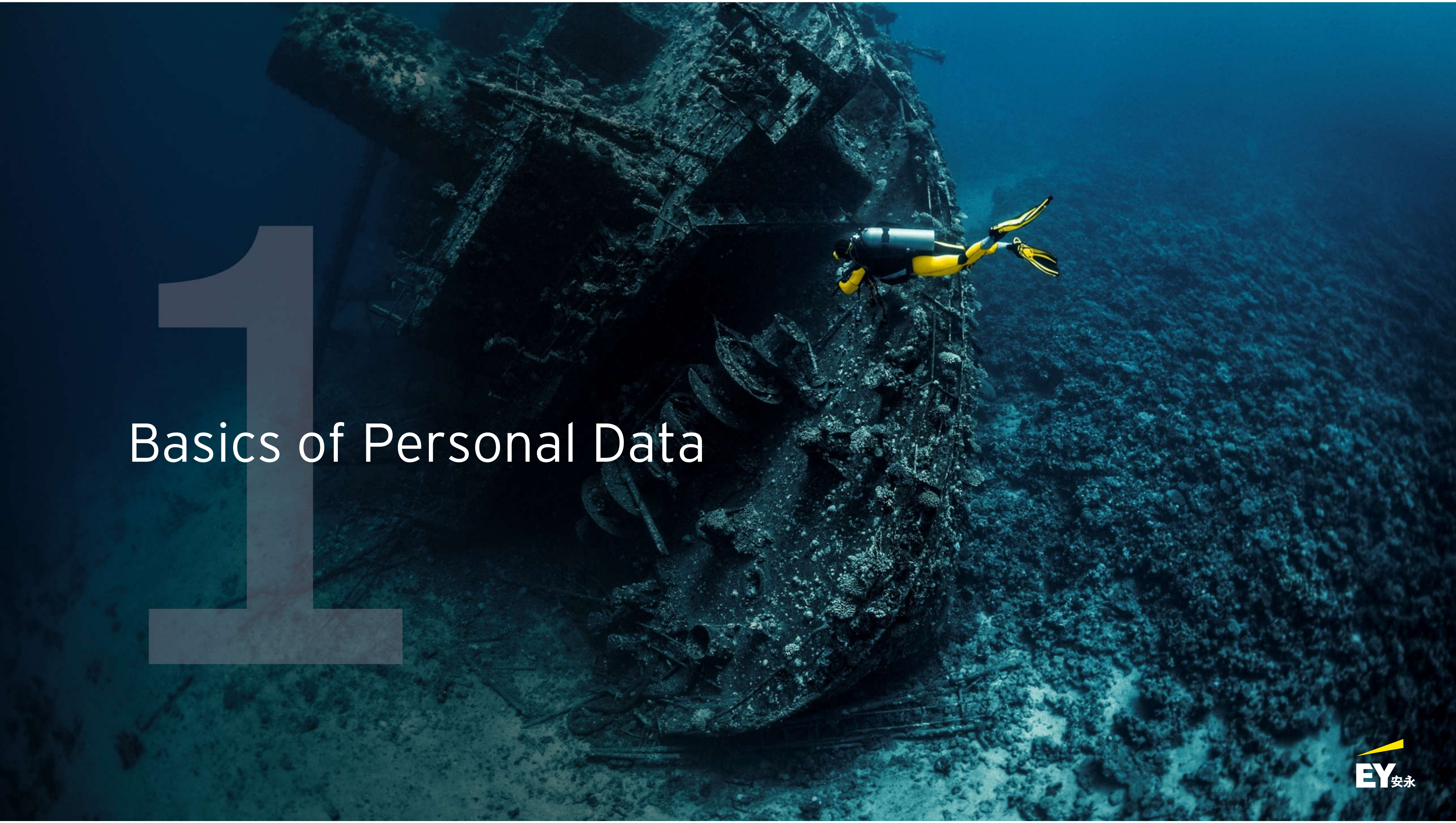
2 Cybersecurity Trends & Statistics

3 General IT Security Controls

4 New Normal - Emerging Cybersecurity Challenges

5 Crisis Management

6 The System and Practices of HKU



1

Basics of Personal Data

Basics of Personal Data

- ‘**Personal data**’ means any data -
  - (a) Relates directly or indirectly to a living individual (“**data subject**”)
    - Can be used to identify that person
  - (b) Exists in a form which can be processed and accessed

    e.g.

Name	**ID card number**
Phone number	**Medical record**
Address	**Employment record**

- **Sensitive personal data**
  - HKID
  - Health-related data
  - Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs
  - Data concerning a person’s sex life or sexual orientation

Basics of Personal Data

- ‘**Data user**’ means a person who
  - Either alone or jointly or in common with other persons, controls the collection, holding, processing, usage
  - Liable as the principal for the wrongful act of its authorized data processor

- ‘**Data processor**’ process data on behalf of the data user, instead of for his/her own purpose(s)
  - Data users are required to, by contractual or other means, ensure that their data processors meet the applicable data privacy requirements

Basics of Personal Data

1 Collection

2 Accuracy & Retention

3 Use

4 Security

5 Openness

6 Data Access & Correction

Basics of Personal Data

1

Collection

Personal data must be collected in a lawful and fair way, for a purpose directly related to a function / activity of the data user. Data collected should be adequate but not excessive.

Basics of Personal Data

2

Accuracy & Retention

Practical steps shall be taken to ensure personal data is accurate and not kept longer than what is necessary to fulfil the purpose for which it is used.

Basics of Personal Data

3

Use

Personal data must be used for the purpose for which the data is collected or for a directly related purpose, unless voluntary and explicit consent with a new purpose is obtained from the data subject.

Basics of Personal Data

4

Security

A data user needs to take practicable steps to safeguard personal data from unauthorized or accidental access, processing, erasure, loss or use.

Basics of Personal Data

5

Openness

A data user must take practicable steps to make personal data policies and practices known to the public regarding the types of personal data it holds and how the data is used.

Basics of Personal Data

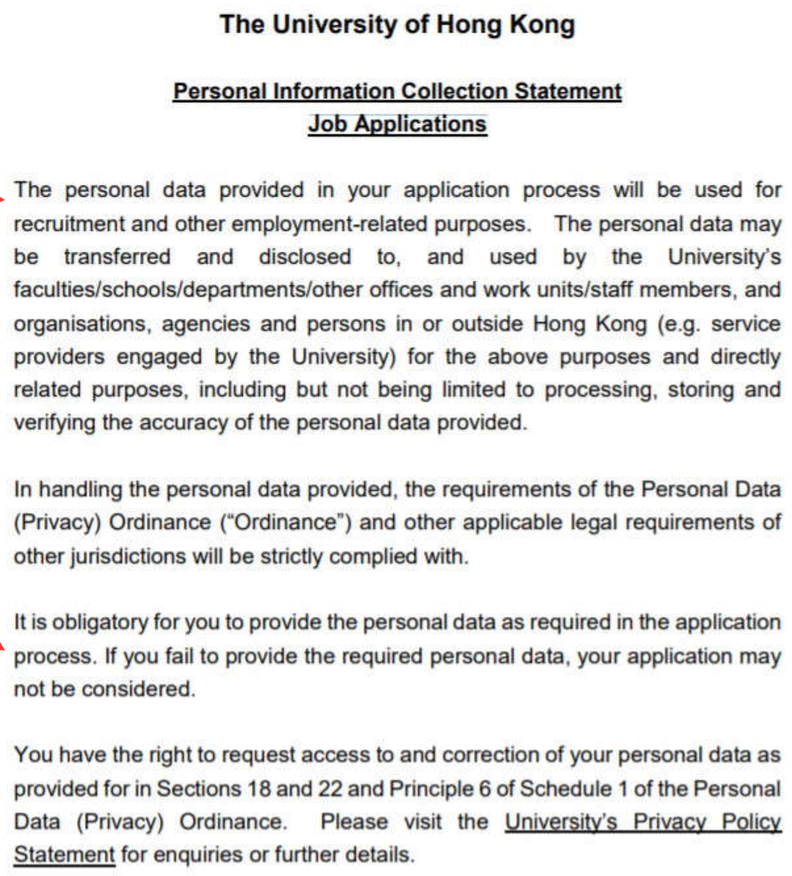
6

Data Access & Correction

A data subject must be given access to his / her personal data and allowed to make corrections if it is inaccurate.

Personal Information Collection Statement (PICS)

1. Statement of Purpose
2. Statement of possible transferees
3. Statement as to whether it is obligatory or voluntary for the individual to supply his personal data
4. Statement of rights of access and correction and contact detail
5. Notice of contact person for requesting access or correction



The University of Hong Kong

Personal Information Collection Statement
Job Applications

The personal data provided in your application process will be used for recruitment and other employment-related purposes. The personal data may be transferred and disclosed to, and used by the University's faculties/schools/departments/other offices and work units/staff members, and organisations, agencies and persons in or outside Hong Kong (e.g. service providers engaged by the University) for the above purposes and directly related purposes, including but not being limited to processing, storing and verifying the accuracy of the personal data provided.

In handling the personal data provided, the requirements of the Personal Data (Privacy) Ordinance ("Ordinance") and other applicable legal requirements of other jurisdictions will be strictly complied with.

It is obligatory for you to provide the personal data as required in the application process. If you fail to provide the required personal data, your application may not be considered.

You have the right to request access to and correction of your personal data as provided for in Sections 18 and 22 and Principle 6 of Schedule 1 of the Personal Data (Privacy) Ordinance. Please visit the University's Privacy Policy Statement for enquiries or further details.

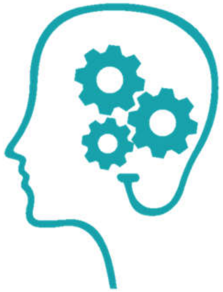
2

Cybersecurity Trends and Statistics

Cybersecurity trends and statistics

- Student PII (personally identifiable information)
- Cutting edge research
- Technology innovations
- Intellectual property

Why would hackers attack an educational institution?



Cybersecurity trends and statistics

- Direct compromise of **email systems**
- Exposure of **sensitive patient information** in school health care systems
- Cyber attacks originating from **foreign countries** to specific entry points within the educational institutions
- **DDoS** attacks that interrupted daily operations during key times in the school year
- Costly **ransomware** that resulted in ransom paid for the return of sensitive data
- **Phishing** attack

Cybersecurity trends and statistics

- Hackers have been targeting universities in an effort **to uncover maritime technology** that is being developed for military use.
- **27 universities** were involved
- Focused on **stealing research data**
- The university networks were breached **with phishing emails** that hackers designed to look like real messages from other universities. The emails were secretly packed with **spyware** instead.
- The effort dates back for almost 2 years

Cybersecurity trends and statistics

Data Breach at one of the major Universities in US

An annual cybersecurity inspection performed by the University revealed vulnerability in a server associated with a database. The information breached included the **names and email addresses** of **355,000 individuals**, including students and teachers of the University.

Cyberattack targeting a University

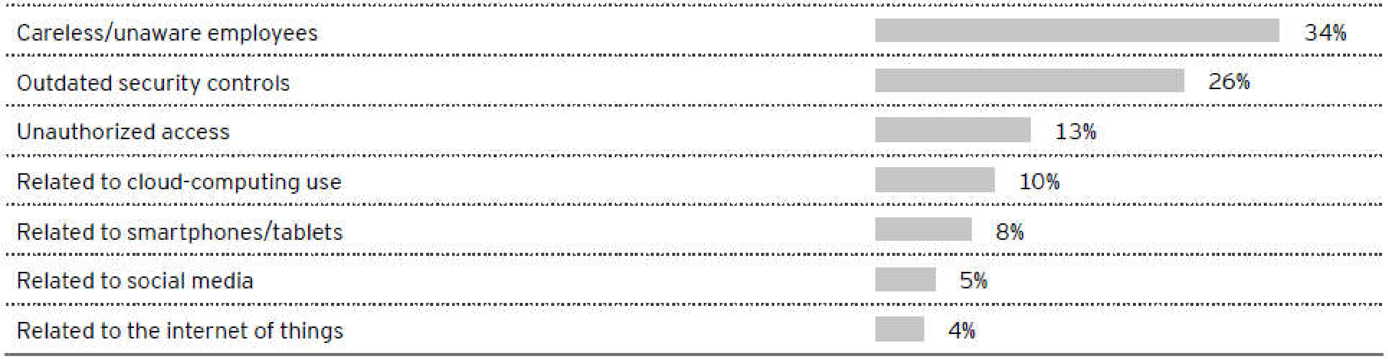
The University experienced a cyberattack exploiting the vulnerability in a software provided by third-party vendor. Over **300,000** unique records with **personal identifiable information (PII)** were involved, including PII from students and employees (names, student ID numbers, addresses, dates of birth, phone numbers, genders etc.), **health and clinical data,** and **study and research data**.

Cybersecurity trends and statistics

- **41%** of **higher education cyber security incidents** and breaches were caused by **social engineering** attacks
- **Phishing scams** → the most prevalent attacks against students, staff and faculty

Human factors

Vulnerabilities with the most increased risk exposure over the past 12 months



34% of the 1,400 organizations that participated the survey see careless/ unaware employees as the biggest vulnerability.

Source: EY Global Information Security Survey

3 General IT Security Controls

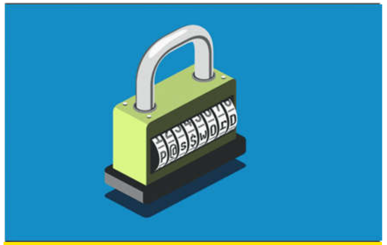
General IT Controls

- System Design and Technology Risk
- System and Network Availability Risk
- End Point Security
- Network Configuration
- IT Security Policies and System Administration Procedures
- Program Change Management
- Patch Management
- Data Security and Privacy
- User Account Management
- Segregation of Duties
- Physical Security and Environment Controls
- Data Backup and Recovery
- Problem and Security Incident Management
- Cloud Management
- Third Party Risk Management

General IT Controls

- **Work Station**
  - **Complex Password**
    - Minimum length of **10** characters
    - Alphanumeric
    - Non-sequential
    - Do not use default password
  - **Lock your computer** when leaving it unattended
  - **Account lockout Policy**
    - Duration: **30 minutes**
    - Threshold: **3 invalid attempts**

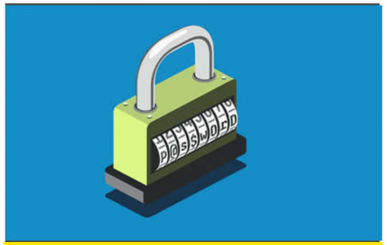
General IT Controls



hacked

6 lowercase letters

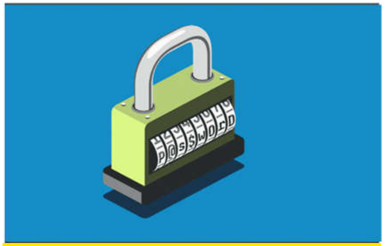
10 MINUTES



HaCKingG

7 lowercase and uppercase letters

23 DAYS



$eCureD1

8 lowercase, uppercase numbers and symbols

463 YEARS

P@ssw0rd

1234567890

12345678

Your name along with your birthday

Starwars

whatever

Letmein

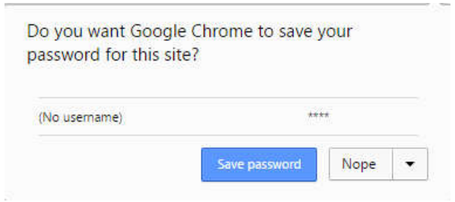
123123

Unlock

football

General IT Controls

- **Avoid using public computer to access confidential files**
  - Public machines can be infected with **key logger malware**
  - **Disable** password saving
  - **Delete** temporary Internet files and browsing history



Do you want Google Chrome to save your password for this site?

(No username) ****

- **Physical Security**
  - Avoid placing workstations in **very public or private locations**
  - **Restrict access** to vulnerable workstations
  - Install **cable locks**
  - Install **privacy screen filters**
  - Loss or destruction of devices should be **reported immediately**

General IT Controls

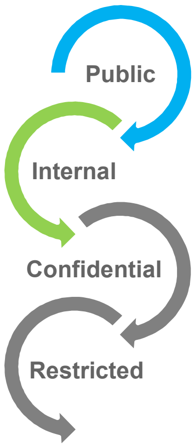
- **Storage**
  - Encryption
  - Organizations that collect **PII** sh a stored on a storage system
  - **Backup** the computer regularly
    - An encrypted disk that crash
  - HKU's **Data Leakage Protectio**
    - A measure adopted by HKU
  - Always encrypt removable medi
    - Store sensitive data only when it is **absolutely necessary** and **erase** the data immediately after using it

DPP4: Data Security

A data user needs to take practicable steps to safeguard personal data from unauthorized or accidental access, processing, erasure, loss or use.

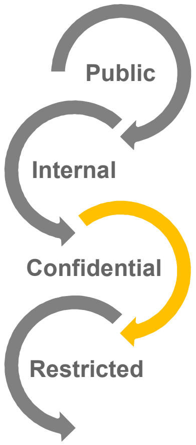
Know what kind of data you are dealing with

- **HKU's Data Classification Scheme**
- **Four Levels of Classification**
  - **Public**
    - Open to public
    - No Restriction on access
    - Present minimal perceived risk
    - i.e. HKU policies, programme information, press releases
  - **Internal**
    - Non-sensitive operational data/information
    - Disclosures are not expected to cause serious harm to HKU
    - Access may be provided to staff based on respective roles and responsibilities
    - i.e. Staff handbooks, training materials, internal procedures



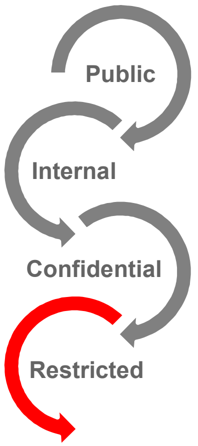
Know what kind of data you are dealing with

- **Confidential**
  - Sensitive data/information intended for use by specific group of authorized personnel within HKU and business partners
  - Assigned on a need-to-use basis
  - Unauthorized disclosure, modification or destruction would adversely affect the business or continuity of operations
  - i.e. Student and staff personal information, unpublished research information, identifiable research subject data



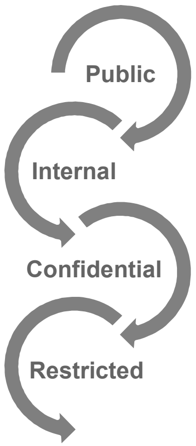
Know what kind of data you are dealing with

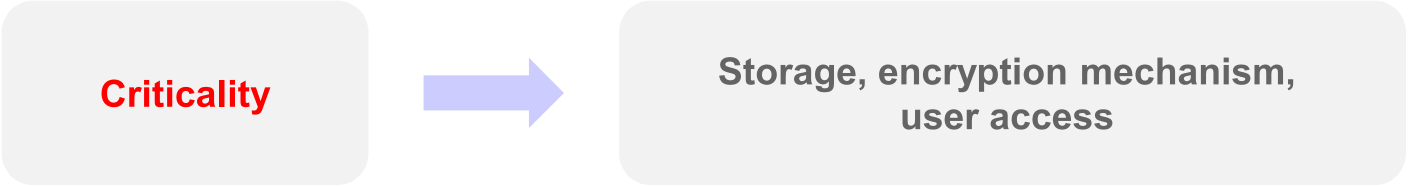
- **Restricted**
  - Data/information that is very sensitive in nature and restricted by HKU, the gov or any other agreements between HKU and 3rd parties
  - Critical to HKU's capacity to conduct its business
  - Used exclusively by limited numbers of predetermined and authorized individuals
  - Financial lost or damage to HKU's reputation
  - i.e. Examination papers before official release, privileged accounts' passwords, sensitive personal data (HKID, credit card information)



Know what kind of data you are dealing with

- Make good use of the **HKU Data / Information Asset Inventory**
  - **Categories**
  - **Description**
  - **Responsible Data Steward**
  - **Concerned Data Custodian**
  - **Physical location**
  - **Digital Storage**
  - **IT Application / System name**
  - **System Owner**
  - **Classification**
  - **Security Measures**





General IT Controls

Follow best practice on user account management

- Formal user account request and review procedure should be in place
- Having a formal **User Access Request Form** can ensure that proper approval have been obtained for all user access requests.
  - The request (application / modification / deletion)
  - Relevant system / application
  - Name and position of the requester
  - Date of submitting the request
  - Name, position and signature of the approver
  - Date of granting the approval
  - Name of the IT Officer who is responsible for the technical procedures
  - Completion date
- **Segregation of Duty** for Requester, Approver and Reviewer
- **Regular review** on the user access list
- Don’t keep an excess amount of testing accounts

General IT Controls

Follow best practice on data backup & recovery

- A critical factor in your backup solution is **remote backups**
- Off-site, or at least off-server, backups will remain viable even if your central server is compromised
- Ensure backups are taken **frequently** and on a **regular** schedule
- Critical data that is continuously updated requires a more frequent backup schedule
- Consider how long you will **retain** each backup based on your business needs
- **Encrypt** the backup files
- Perform **backup recovery test** on a regular basis

General IT Controls

Patch servers, workstations and relevant applications up-to-date to avoid known vulnerabilities being exploited

- Regular checking on available patches from vendor / emails from ITS
- Test the patches before deploying to production environment
- Regular patch scanning to identify gaps

Do not expose unnecessary service to user

- Only allow minimum permission under the least privilege basis
- Restrict normal users from installing or uninstalling software
- Regular checking on the application and services running
- Well defined firewall rule set

Emerging Cybersecurity & Data Privacy Challenges

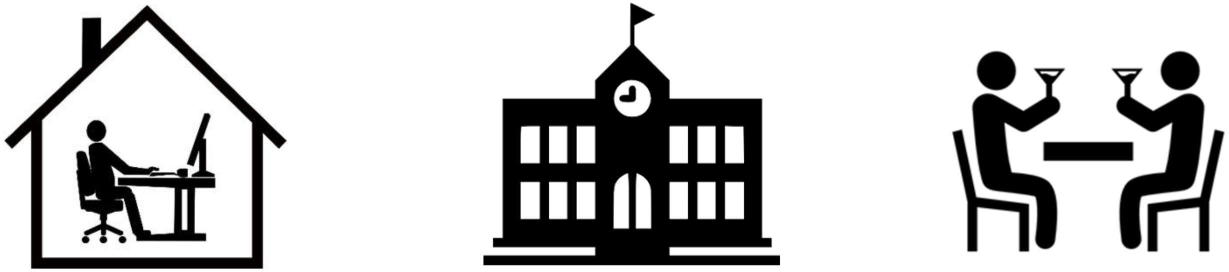
New Normal

COVID-19

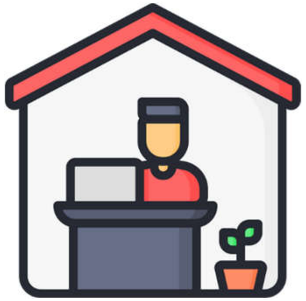
The COVID-19 pandemic has popularized the use of this term.

“A state to which a ***society****,* ***economy****,* ***technological environment*** *etc. settles following a crisis, which differ from the situation that prevailed prior to the start of the crisis.”*

The pandemic has changed the daily life for most people, such as limiting person-to-person contact, social distancing etc.



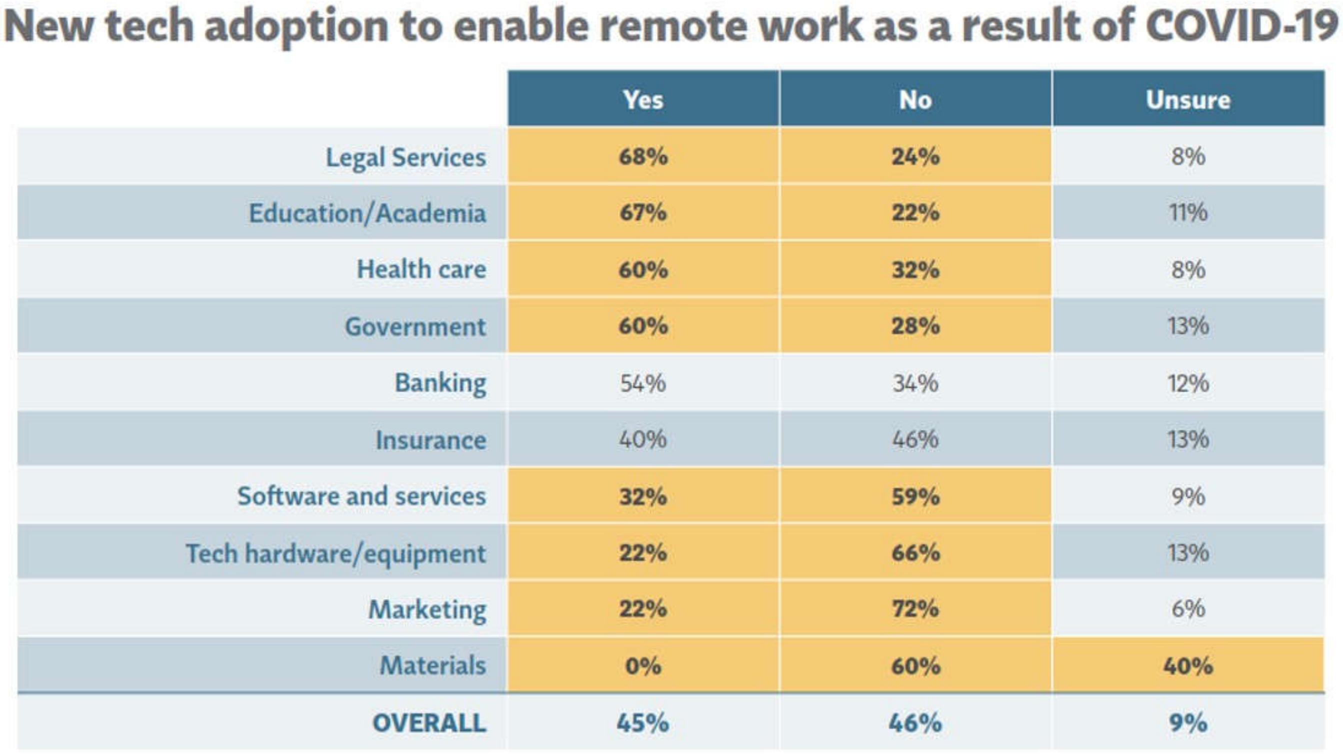
Covid-19 Pandemic introduced…



Work-From-Home

WFH Overview

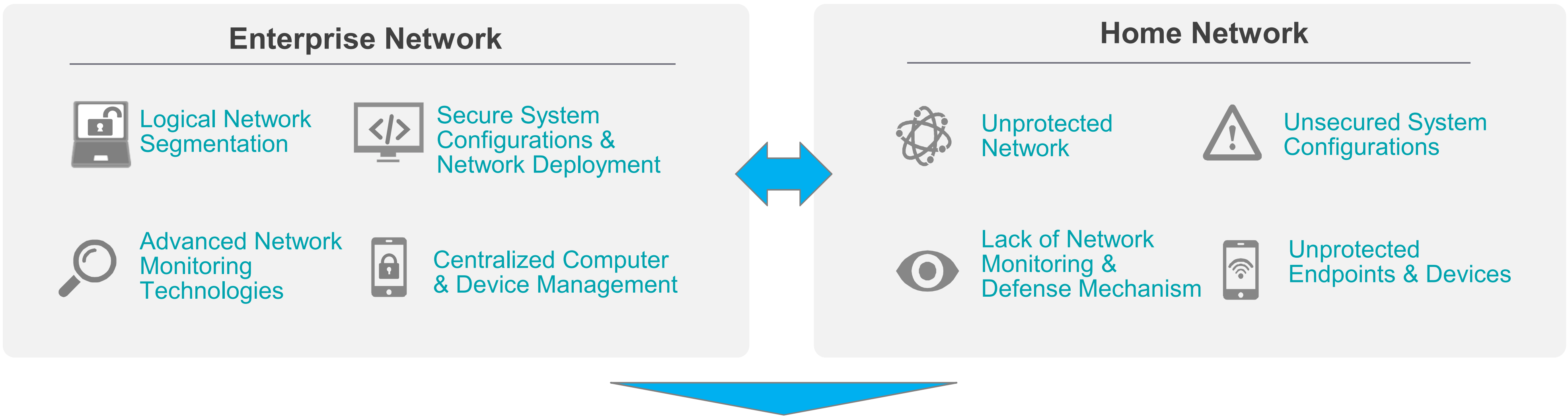
- Education/academia has been one of the biggest new adopters of WFH technologies



New tech adoption to enable remote work as a result of COVID-19

	Yes	No	Unsure
Legal Services	68%	24%	8%
Education/Academia	67%	22%	11%
Health care	60%	32%	8%
Government	60%	28%	13%
Banking	54%	34%	12%
Insurance	40%	46%	13%
Software and services	32%	59%	9%
Tech hardware/equipment	22%	66%	13%
Marketing	22%	72%	6%
Materials	0%	60%	40%
OVERALL	45%	46%	9%

Difference between WFH and office



Enterprise Network

- Logical Network Segmentation
- Secure System Configurations & Network Deployment
- Advanced Network Monitoring Technologies
- Centralized Computer & Device Management

Home Network

- Unprotected Network
- Unsecured System Configurations
- Lack of Network Monitoring & Defense Mechanism
- Unprotected Endpoints & Devices

Major Risks Arising from Work From Home Arrangement

- More likely to be infected by malware due to relatively unsecured system configurations
- Higher chance of being compromised by external cyber-attackers due to insufficient network protection and the lack of the network monitoring
- Higher likelihood of accidental data leakage due to less secure endpoint protection in home network

Bring Your Own Device & Video Conferencing

- **Bring Your own Device (BYOD)**
  - Employees use their personal devices to access work-related systems and the organization’s information, potentially personal or confidential data.

- **Video Conferencing**
  - A technology that allows users in different locations to hold face-to-face meetings without having to move to a single location together.

Company Meeting

Seminar

Remote classroom

zoom

Webex Meetings

BYOD Security Risks

- BYOD
  - A lot of personal devices are already infected with **malware**
  - **Security configurations** and **hardening controls** might not be aligned with the organization’s standards
  - Storing the **organization’s information and data** on personal devices without proper guidelines and controls might lead to various **privacy issue** (i.e. data retention)

  - **Unsecured** and **uncontrolled** BYOD devices might create huge security loopholes in the organization’s security posture

BYOD Security Tips

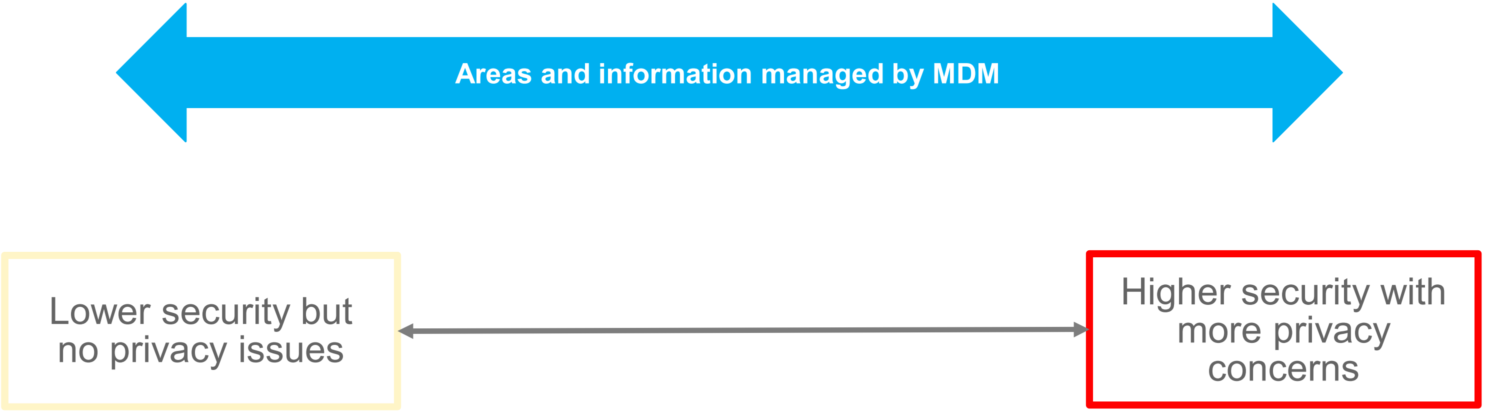
- Establish a **BYOD Policy** outlining critical security considerations such as:
  - Onboarding procedures
  - Type of devices that are sanctioned by the organization
  - Employees who can leverage BYOD
  - Data that can be accessed from these devices

- Use **Mobile Device Management (MDM)** solutions to control and monitor the devices:
  - Monitor the applications and updates being installed on the device
  - Deploy update patches
  - Monitor the usage of devices in the MDM server
  - Configure security settings on the device
  - Track the device's location
  - Remote wipe the device

- It's very important for the organization to ascertain if personal/sensitive data should be retained in BYOD devices and how its **retention** and **erasure policy** can be applied equally and effectively

BYOD Security Tips

- Whilst a certain level of monitoring and control should be maintained over the BYOD devices, **both the organization and the users** should be aware of **what** and **how** the device is being managed


Areas and information managed by MDM
Lower security but no privacy issues
Higher security with more privacy concerns

Video Conferencing Security Risks

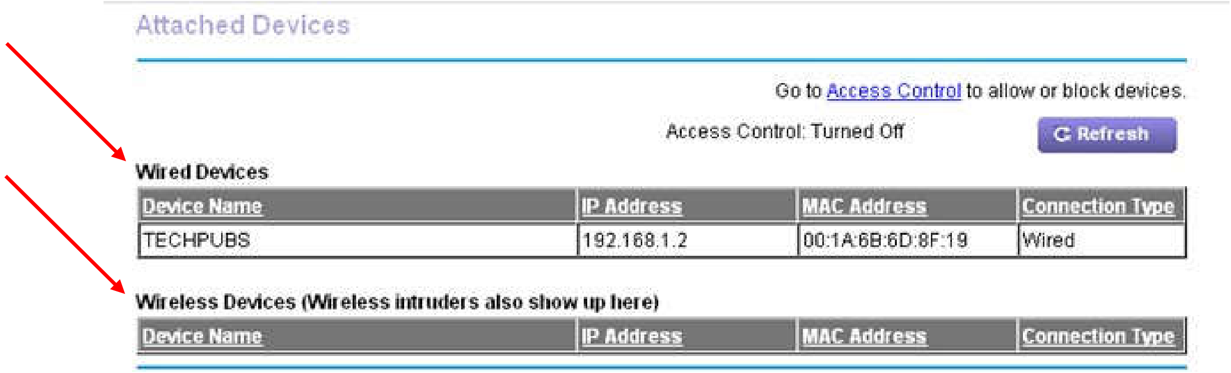
- Unauthorized access to private meetings
- Data transmission that isn’t secure
- Users spreading malicious links or files on the chatroom
- Hackers potentially uploading video conferencing credentials on the dark web, putting a company’s sensitive and business critical information at risk of exposure.
- Accidental sharing of sensitive footage or information

Video Conferencing Security Tips

- **Passwords** should be used for proper access control
- “**Waiting room**” feature should be leveraged such that the host can **admit or remove** attendees attempting to access the video conference
- Only use video conferencing tools that support **end-to-end encryption**
- Perform **routine updates** of all video conferencing tools to **patch vulnerabilities**
- Use **properly licensed** video conferencing tools
- Pay **extra attention** when you are **sharing** your screen
- **Mute** the microphone / **turnoff the video** when necessary

Work-From-Home security tips

- Check if your home's network has been **hijacked** by unauthorized users
  - Start by checking if there is any unknown wired or wireless devices connected to the network



Attached Devices

Go to Access Control to allow or block devices.

Access Control: Turned Off

Wired Devices

Device Name	IP Address	MAC Address	Connection Type
TECHPUBS	192.168.1.2	00:1A:6B:6D:8F:19	Wired

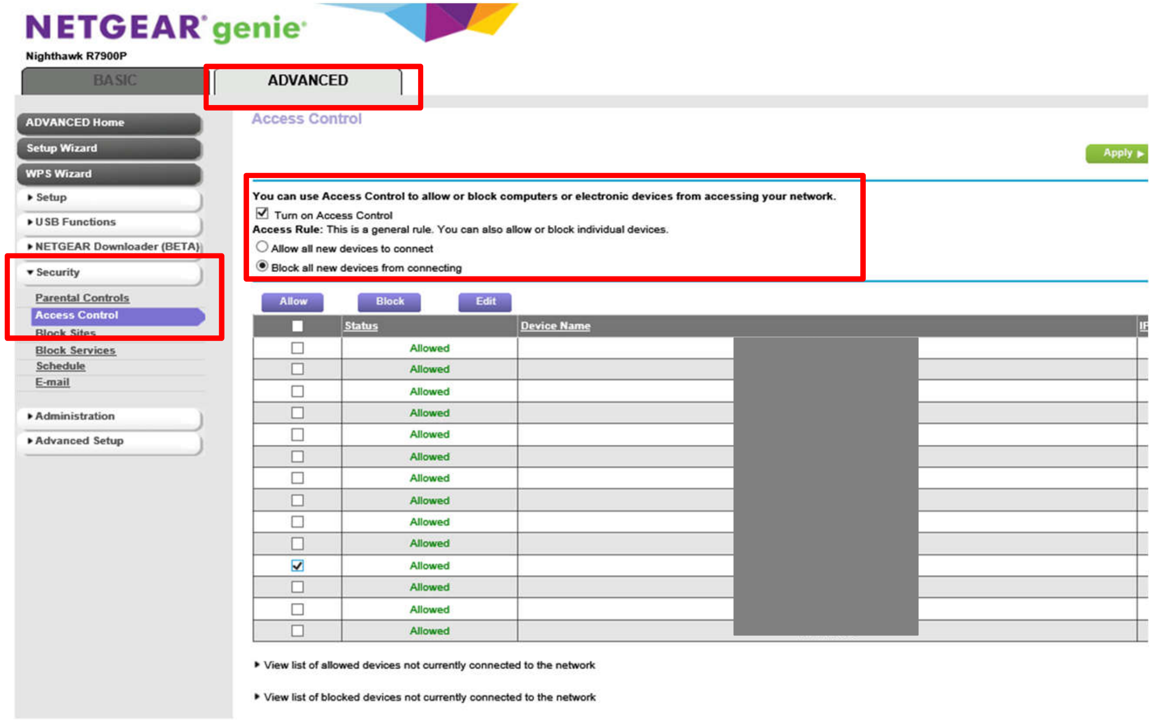
Wireless Devices (Wireless intruders also show up here)

Device Name	IP Address	MAC Address	Connection Type

- Secure your router – change the **Wi-Fi password** and **network name (SSID)**

Work-From-Home security tips

- Use **MAC address filtering** or other **access control** to define a list of trusted devices and only allow these devices to connect to your Wi-Fi network



You can use Access Control to allow or block computers or electronic devices from accessing your network.

☑ Turn on Access Control

Access Rule: This is a general rule. You can also allow or block individual devices.

○ Allow all new devices to connect

● Block all new devices from connecting

■	Status	Device Name
□	Allowed	[redacted]
□	Allowed	[redacted]
□	Allowed	[redacted]
□	Allowed	[redacted]
□	Allowed	[redacted]
□	Allowed	[redacted]
□	Allowed	[redacted]
□	Allowed	[redacted]
□	Allowed	[redacted]
□	Allowed	[redacted]
☑	Allowed	[redacted]
□	Allowed	[redacted]
□	Allowed	[redacted]
□	Allowed	[redacted]

- View list of allowed devices not currently connected to the network
- View list of blocked devices not currently connected to the network

Source: NETGEAR: https://kb.netgear.com/23289/How-do-I-configure-Access-Control-or-MAC-Filtering-on-my-NETGEAR-router-using-the-router-web-interface

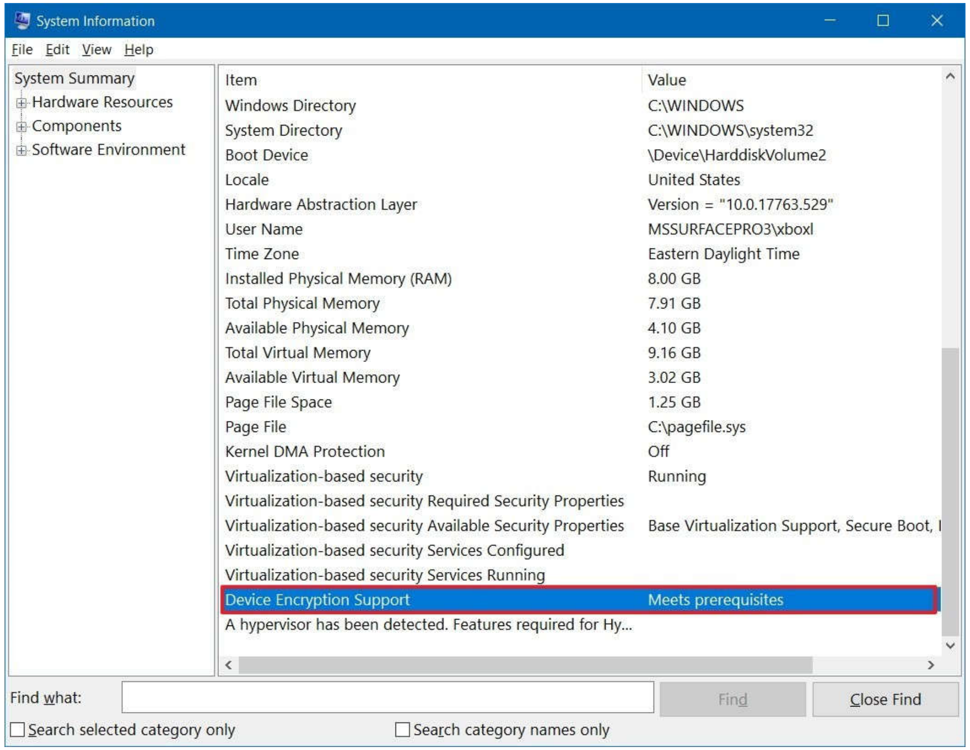
Work-From-Home security tips

- **Secure your device**
  - **Device encryption** protects your data from unauthorized access in case your device is lost or stolen
  - The entire system drive will be **scrambled** upon the activation of this feature and the data can only be accessed with the correct password

Work-From-Home security tips

► Check whether your device meets the hardware requirements for device encryption

- Check the item “Device Encryption Support”
- If it displays “Meets prerequisites”, then your Windows devices support file encryption



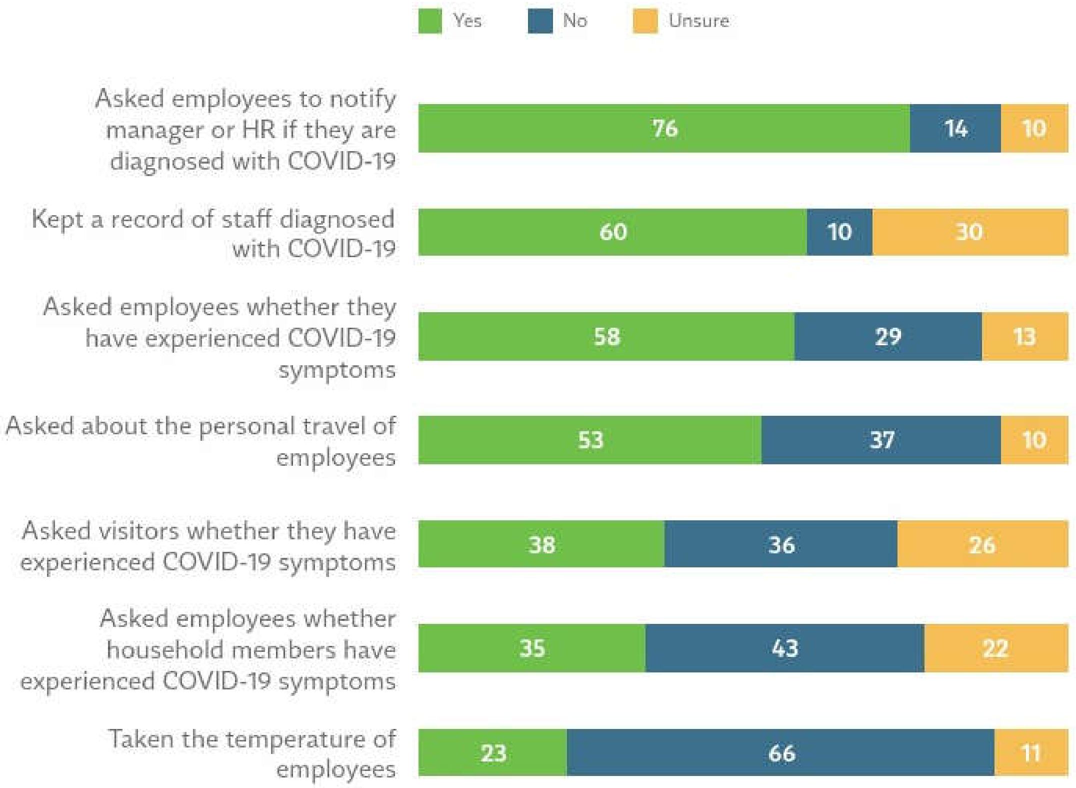
Item	Value
Windows Directory	C:\WINDOWS
System Directory	C:\WINDOWS\system32
Boot Device	\Device\HarddiskVolume2
Locale	United States
Hardware Abstraction Layer	Version = "10.0.17763.529"
User Name	MSSURFACEPRO3\xboxl
Time Zone	Eastern Daylight Time
Installed Physical Memory (RAM)	8.00 GB
Total Physical Memory	7.91 GB
Available Physical Memory	4.10 GB
Total Virtual Memory	9.16 GB
Available Virtual Memory	3.02 GB
Page File Space	1.25 GB
Page File	C:\pagefile.sys
Kernel DMA Protection	Off
Virtualization-based security	Running
Virtualization-based security Required Security Properties	
Virtualization-based security Available Security Properties	Base Virtualization Support, Secure Boot, I
Virtualization-based security Services Configured	
Virtualization-based security Services Running	
Device Encryption Support	Meets prerequisites
A hypervisor has been detected. Features required for Hy...	

Work-From-Home security tips

- Enable Anti-virus protection on the devices
- Pay attention to the OS End-Of-Life
- Delete and manage cookies
- Disable web browser’s automatic password saving
- Disable plug-ins
- Update the web browser regularly
- VPN
- Keep work data on work computers
- Block the sight lines / install privacy filters
- Keep your device close to you
- Don’t use random thumb drives

Data Privacy – Employee Health Data

- Most organizations have collected data from employees about COVID-19 symptoms and kept diagnostic records



Data Privacy – Employee Health Data

- Organizations would inevitably collect, use, process or retain additional personal data (i.e. health data) to protect the community from serious threats to public health.

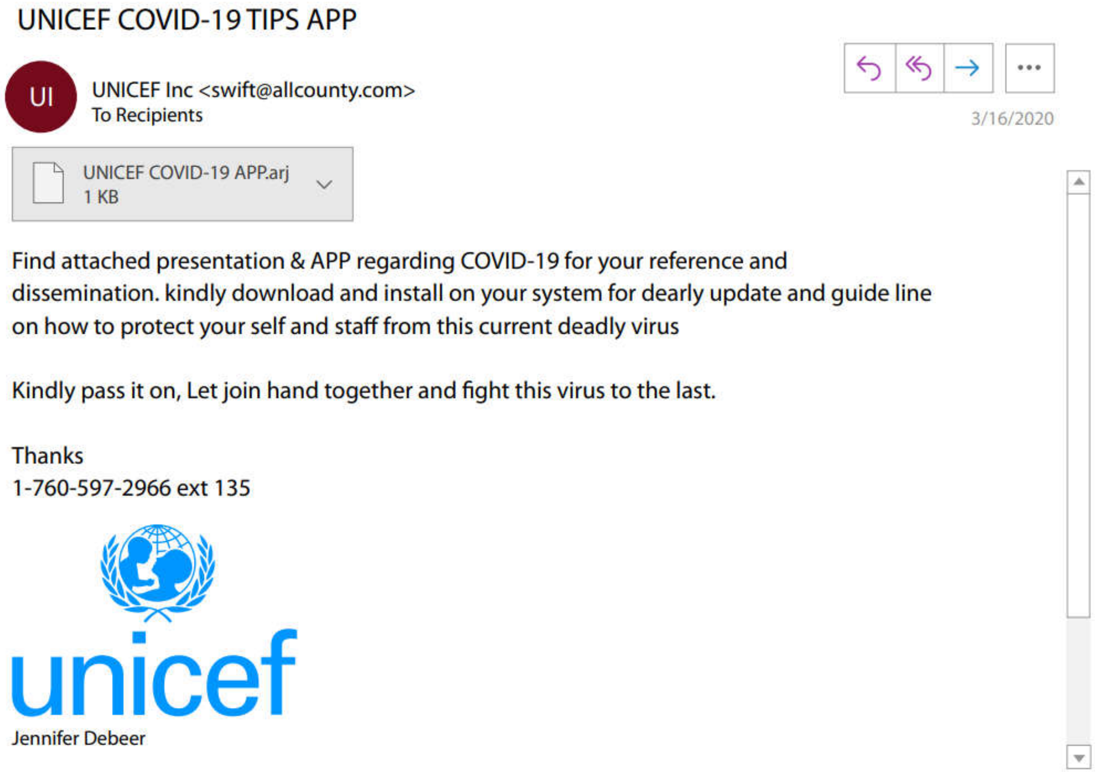
Best Practice

- Avoid asking for/providing excessive medical data
- Pay attention to the purpose of collection and class of person to whom the data may be transferred to
- Conduct privacy and security reviews and data protection impact assessment
- Provide data privacy guideline to relevant personnel

Social Engineering

- Dispersed workforce during WFH → Increased telecommunication → More exposed to phishing attacks
- Using the fear of COVID-19 as the theme for their malicious activities and spread various malware through phishing emails
- Malwares provide attackers with access to infected systems:
  - Remote desktop access
  - Remote webcam control
  - Password stealer
  - Keylogger
  - Remote shell
  - Privilege escalation
  - System manipulation

Social Engineering – phishing email



UNICEF COVID-19 TIPS APP

UNICEF Inc <swift@allcounty.com>
To Recipients

3/16/2020

UNICEF COVID-19 APP.arj
1 KB

Find attached presentation & APP regarding COVID-19 for your reference and dissemination. kindly download and install on your system for dearly update and guide line on how to protect your self and staff from this current deadly virus

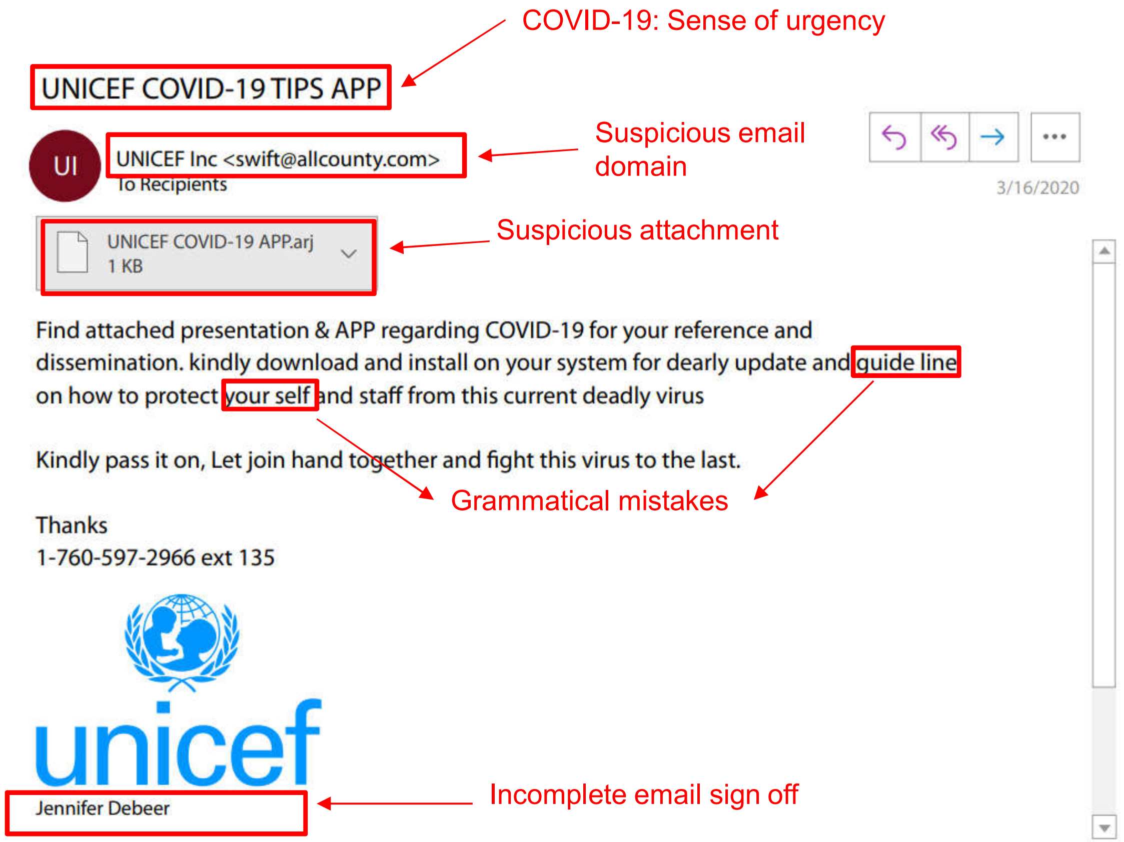
Kindly pass it on, Let join hand together and fight this virus to the last.

Thanks
1-760-597-2966 ext 135

Jennifer Debeer

Source: Enduring from home: COVID-19's impact on business security, Malwarebytes 2020

Social Engineering – phishing email



UNICEF COVID-19 TIPS APP

UI UNICEF Inc <swift@allcounty.com>
To Recipients

3/16/2020

UNICEF COVID-19 APP.arj
1 KB

Find attached presentation & APP regarding COVID-19 for your reference and dissemination. kindly download and install on your system for dearly update and guide line on how to protect your self and staff from this current deadly virus

Kindly pass it on, Let join hand together and fight this virus to the last.

Thanks
1-760-597-2966 ext 135

unicef
Jennifer Debeer

COVID-19: Sense of urgency

Suspicious email domain

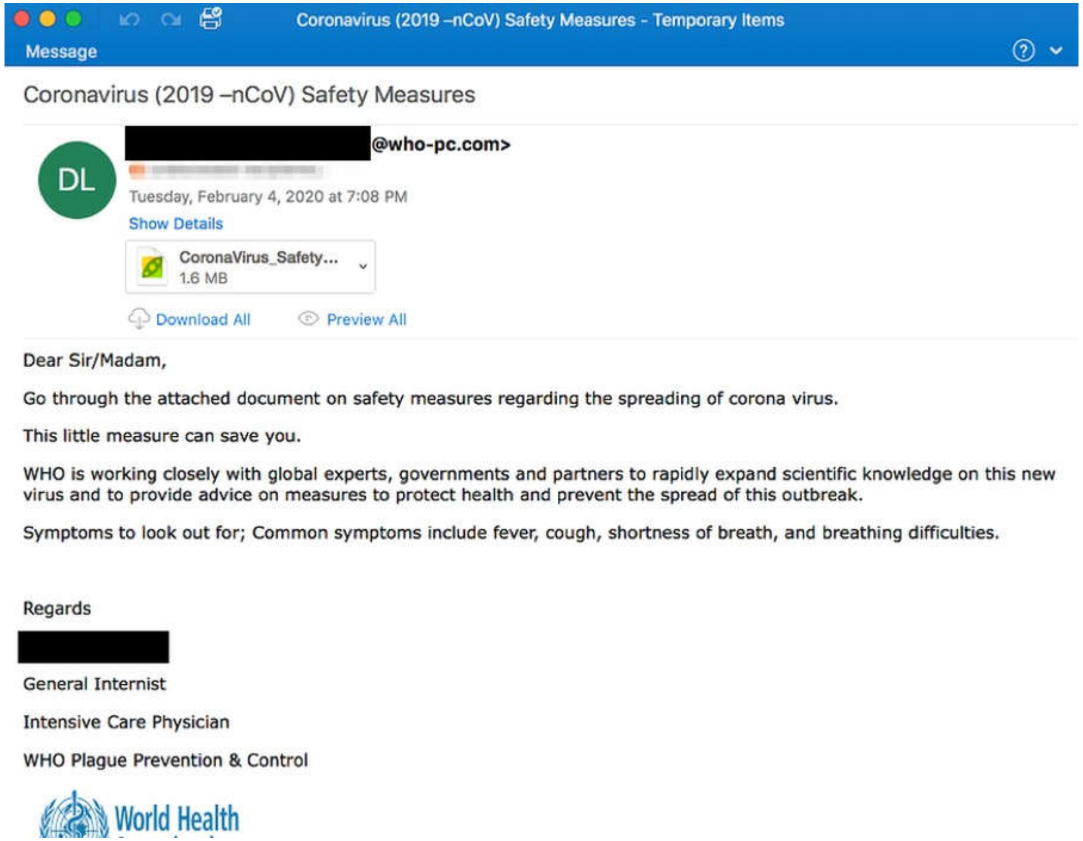
Suspicious attachment

Grammatical mistakes

Incomplete email sign off

Source: *Enduring from home: COVID-19's impact on business security, Malwarebytes 2020*

Social Engineering – phishing email



Coronavirus (2019 –nCoV) Safety Measures

DL [redacted]@who-pc.com>

Tuesday, February 4, 2020 at 7:08 PM

CoronaVirus_Safety...
1.6 MB

Dear Sir/Madam,

Go through the attached document on safety measures regarding the spreading of corona virus.

This little measure can save you.

WHO is working closely with global experts, governments and partners to rapidly expand scientific knowledge on this new virus and to provide advice on measures to protect health and prevent the spread of this outbreak.

Symptoms to look out for; Common symptoms include fever, cough, shortness of breath, and breathing difficulties.

Regards

[redacted]

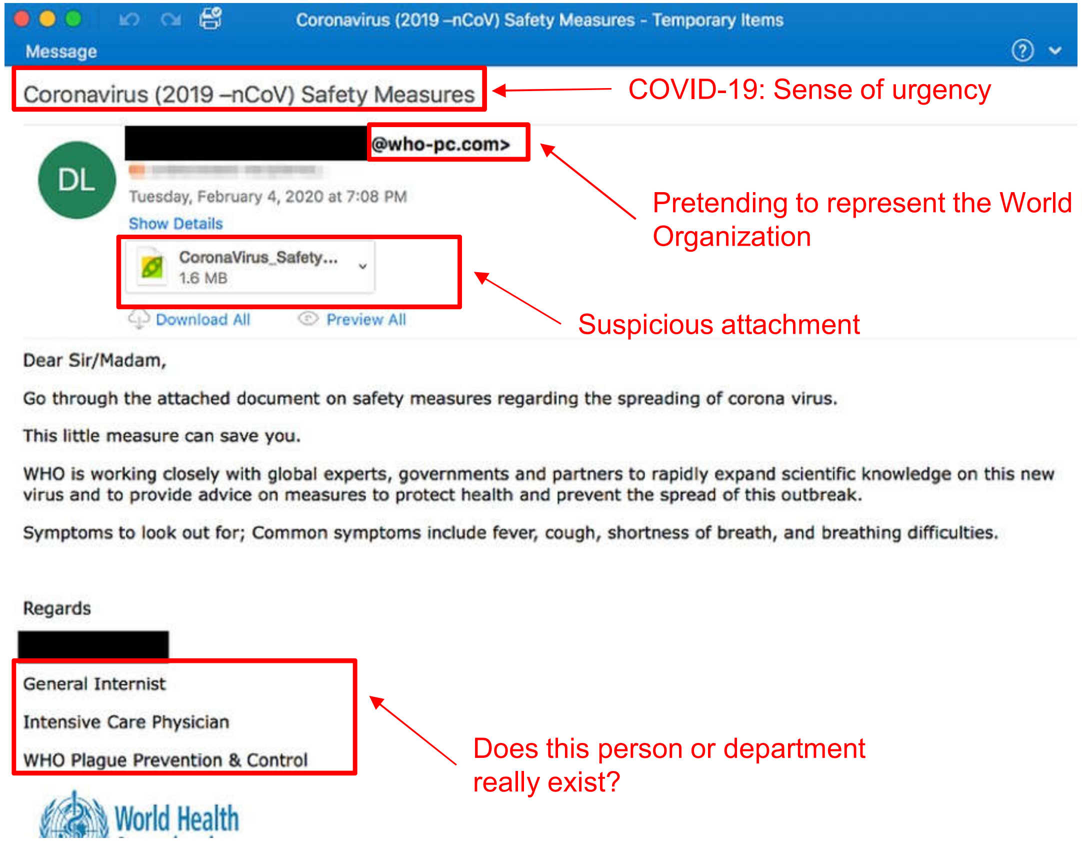
General Internist

Intensive Care Physician

WHO Plague Prevention & Control

Source: https://www.bbc.com/news/technology-51838468

Social Engineering – phishing email



Coronavirus (2019 –nCoV) Safety Measures

[redacted]@who-pc.com>

Tuesday, February 4, 2020 at 7:08 PM

Show Details

CoronaVirus_Safety... 1.6 MB

Dear Sir/Madam,

Go through the attached document on safety measures regarding the spreading of corona virus.

This little measure can save you.

WHO is working closely with global experts, governments and partners to rapidly expand scientific knowledge on this new virus and to provide advice on measures to protect health and prevent the spread of this outbreak.

Symptoms to look out for; Common symptoms include fever, cough, shortness of breath, and breathing difficulties.

Regards

[redacted]

General Internist

Intensive Care Physician

WHO Plague Prevention & Control

COVID-19: Sense of urgency

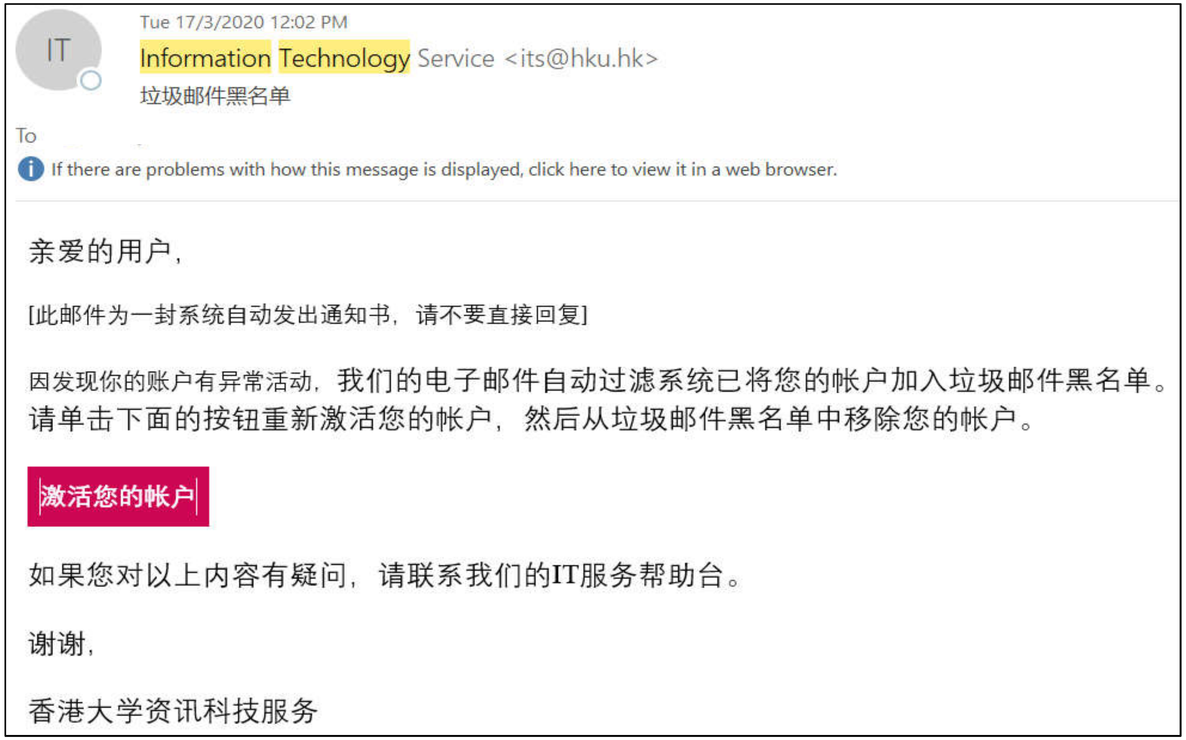
Pretending to represent the World Health Organization

Suspicious attachment

Does this person or department really exist?

Source: https://www.bbc.com/news/technology-51838468

Social Engineering – phishing email



Tue 17/3/2020 12:02 PM

Information Technology Service <its@hku.hk>

垃圾邮件黑名单

To

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

亲爱的用户,

[此邮件为一封系统自动发出通知书，请不要直接回复]

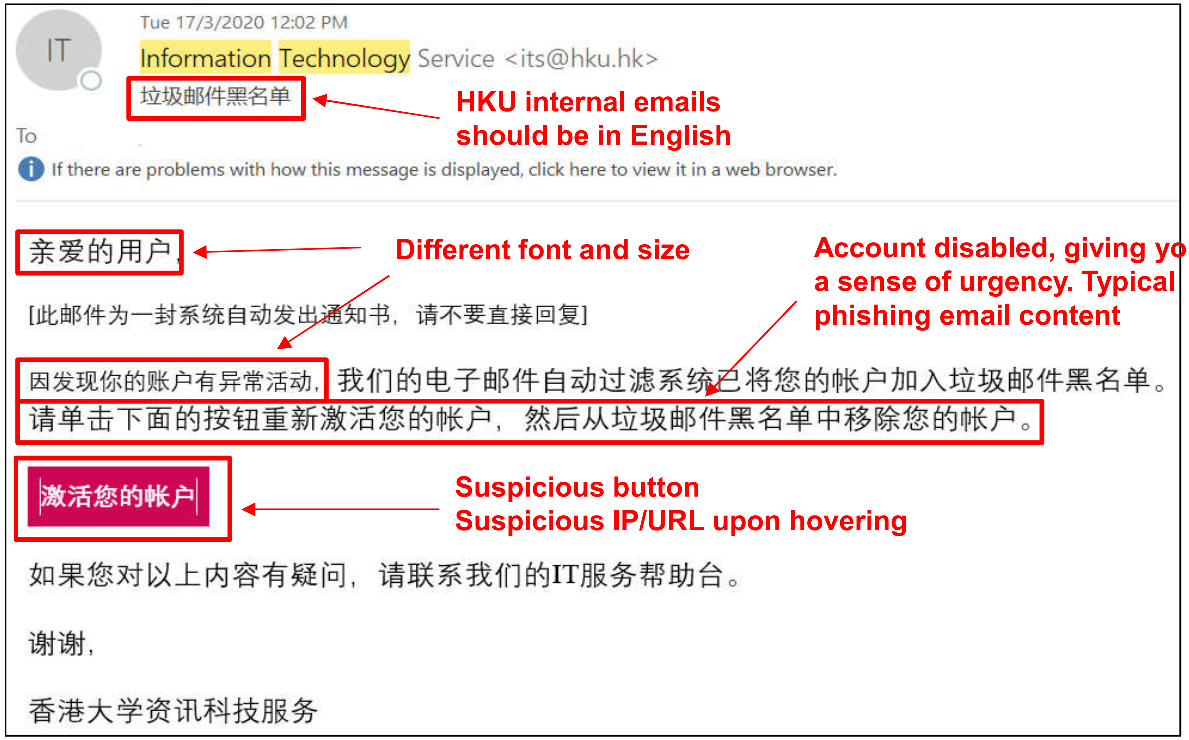
因发现你的账户有异常活动，我们的电子邮件自动过滤系统已将您的帐户加入垃圾邮件黑名单。请单击下面的按钮重新激活您的帐户，然后从垃圾邮件黑名单中移除您的帐户。

如果您对以上内容有疑问，请联系我们的IT服务帮助台。

谢谢,

香港大学资讯科技服务

Social Engineering – phishing email



Tue 17/3/2020 12:02 PM

Information Technology Service <its@hku.hk>

垃圾邮件黑名单

To

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

亲爱的用户,

[此邮件为一封系统自动发出通知书，请不要直接回复]

因发现你的账户有异常活动，我们的电子邮件自动过滤系统已将您的帐户加入垃圾邮件黑名单。请单击下面的按钮重新激活您的帐户，然后从垃圾邮件黑名单中移除您的帐户。

如果您对以上内容有疑问，请联系我们的IT服务帮助台。

谢谢，

香港大学资讯科技服务

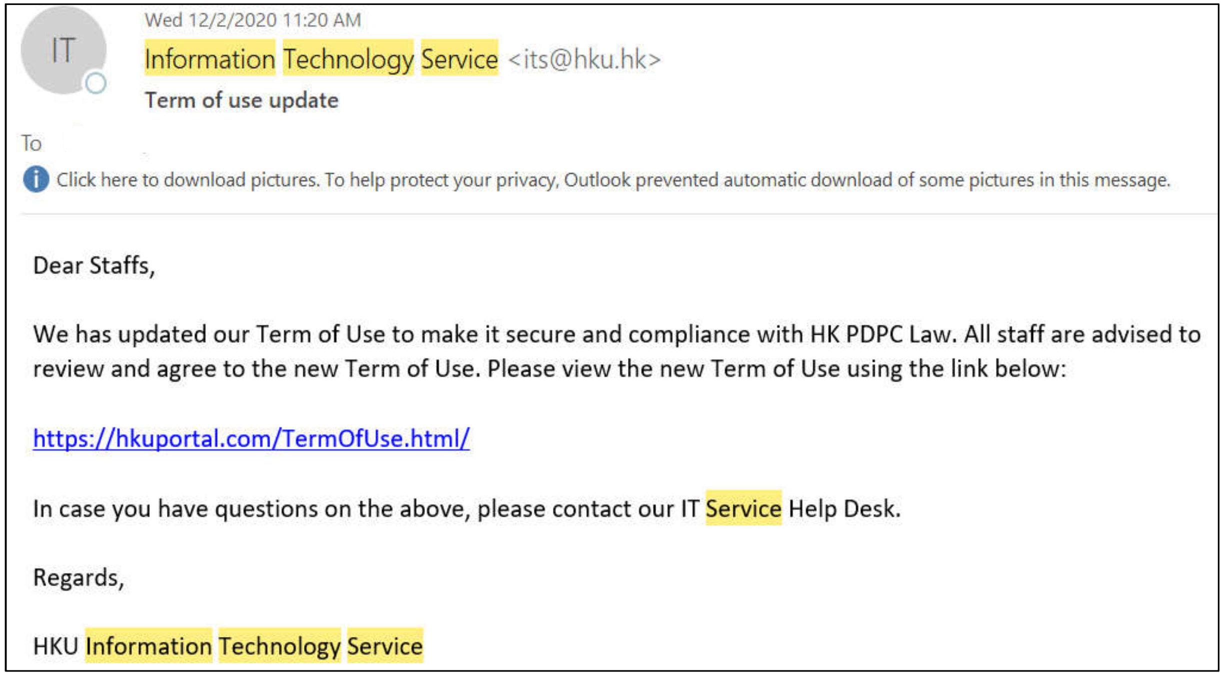
HKU internal emails should be in English

Different font and size

Account disabled, giving you a sense of urgency. Typical phishing email content

Suspicious button
Suspicious IP/URL upon hovering

Social Engineering – phishing email



Wed 12/2/2020 11:20 AM

Information Technology Service <its@hku.hk>

Term of use update

To

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Dear Staffs,

We has updated our Term of Use to make it secure and compliance with HK PDPC Law. All staff are advised to review and agree to the new Term of Use. Please view the new Term of Use using the link below:

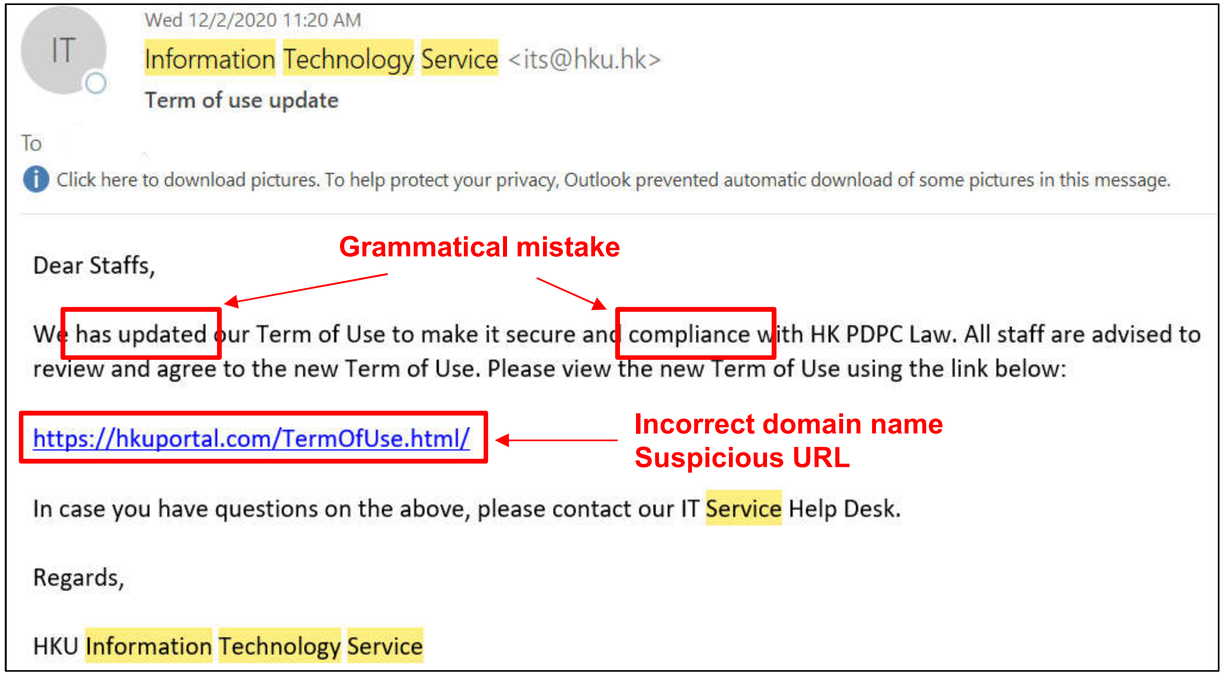
https://hkuportal.com/TermOfUse.html/

In case you have questions on the above, please contact our IT Service Help Desk.

Regards,

HKU Information Technology Service

Social Engineering – phishing email



Wed 12/2/2020 11:20 AM

Information Technology Service <its@hku.hk>

Term of use update

To

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Dear Staffs,

We has updated our Term of Use to make it secure and compliance with HK PDPC Law. All staff are advised to review and agree to the new Term of Use. Please view the new Term of Use using the link below:

https://hkuportal.com/TermOfUse.html/

In case you have questions on the above, please contact our IT Service Help Desk.

Regards,

HKU Information Technology Service

Social Engineering – phishing email

Be Aware . Be Secure

- **Spelling errors** (e.g., “pessward”), lack of punctuation or poor grammar.
- **Hyperlinked URL** differs from the title name displayed, the link is shortened.
- **Sense of urgency.** Phishing emails will usually use a language that demands for immediate actions.
- **Personally Identifiable Information.** Requests for personal information like user credential, financial transactions.
- **Suspicious attachment.** Request to open attachments to check and verify data.
- **Forged sender identity.** The email address domain and email sign off do not match with the claimed identity.

Social Engineering – dumpster diving

☞ **SHRED** - Any document which is of no use to you, shred them before throwing away into the bin!

☞ **DESTROY** - If you are getting rid of any electronics (USB drive, old phones, hard disks, make sure your wipe off the data and physically destroy the same before dumping them

Documents from work

Bills – telephone, internet, electricity, chemist, hospital

Financials – insurance premium notice, new policy, credit card statement, offers

Postal address on parcels, couriers etc.

5 Crisis Management

Crisis Management – What to do in case of data breach?

- C.A.R.E
  - **C**ontaining the data breach to prevent further compromise of personal data
  - **A**ssessing the data breach by gathering the facts and evaluating the risks, including the harm to affected individuals. Where assessed to be necessary, continuing efforts should be made to prevent further harm even as the organization proceeds to implement full remedial action.
  - **R**eporting the data breach to all affected individuals and the PCPD, if necessary.
  - **E**valuating the organization's response to the data breach incident and consider the actions which can be taken to prevent future data breaches. Remediation efforts may continue to take place at this stage.

Crisis Management - Contain

- **C.A.R.E**
  - An organization should act swiftly as soon as it is aware of a data breach.
  - An assigned individual should activate the response team to reduce the potential impact of the data breach.
  - An initial assessment should be conducted to determine the severity of the data breach.

- **Cause of the data breach and whether it is still ongoing**
- **Number of affected individuals**
- **Types of personal data involved**
- **The affected systems and services**
- **Whether external assistance is required to contain the breach**

Crisis Management - Contain

- **C.A.R.E**
  - The assessment allows organizations to decide on the immediate actions to be taken.

- **Isolate the compromised system from the Internet or network**
- **Prevent further unauthorized access to the system. Reset passwords and change the access rights to the compromised system, where applicable.**
- **Stop the identified practices that led to the data breach**
- **Establish whether the lost data can be recovered and steps that can be taken to minimize any harm or impact caused by the data breach**

  - Evidence of the data breach and post-breach response should be kept and recorded in an Incident Log respectively to facilitate follow-up investigations.

Crisis Management - Assess

- C.A.R.E
  - Upon the containment of the data breach, an in-depth assessment should be conducted to identify and limit the impact and damage.

    - **Context of the data breach**
    - **Ease of identifying individuals from the compromised data**
    - **Circumstances of the data breach**

  - The in-depth assessment should allow organizations to conclude whether the data breach is likely to result in significant impact to the affected individuals.
  - Organizations can take steps to reduce any potential harm to the affected individuals.

Crisis Management - Report

- **C.A.R.E**
  - Organizations should have in place appropriate processes to notify the affected individuals and the PCPD, if necessary.

    - **Who needs to be notified?**
    - **How should the affected individuals be notified?**
    - **What details should be included in the notification?**
    - **When should the notification be done?**

  - If a data user decides to report a data breach to the Privacy Commissioner, the data user may complete a Data Breach Notification Form and submit the completed form online, by fax, in person or by post.

Crisis Management - Evaluate

- C.A.R.E
  - The organization should review and learn from the data breach incident to improve its personal data handling practices and prevent the reoccurrence of similar incidents.

    - **Data breach management plan and response**
    - **Existing measures and processes**
    - **Roles of external parties**

  - Regular trainings should be provided to all employees so as to raise their overall security awareness.

Five Guiding Principles

Protect what matters most

Manage cybersecurity risk at the right level

Provide the right access at the right time

Recover quickly and securely

Practice proactive cybersecurity

The System & Practices of HKU

The System & Practices of HKU

- Information Security and Data Management Policy: https://isdm.hku.hk/
- The Privacy Policy Statement: http://www.hku.hk/privacy_policy/
- Code of Practice (revised version 2019): https://intraweb.hku.hk/reserved_1/gsabc/pdpo_cop.pdf (portable storage devices, incident handling / reporting and other guidelines)

The University of Hong Kong

The System & Practices of HKU

- Data Collection Statement
- Statutory Data Access / Correction Request Process
- Central Compliance Team (compliance/monitoring)
- University Data Protection Officer and Personal Data Protection Coordinators
- Information Technology Services (advice / security measures / guidelines / training information):

  https://www.its.hku.hk/services/training/infosec/personal-data-protection

The University of Hong Kong

The System & Practices of HKU

The Public Expectation

Awareness and Education

GOOD PRACTICE

The University of Hong Kong

EY | Assurance | Tax | Transactions | Consulting

About EY
EY is a global leader in assurance, tax, transaction and consulting services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com