Modules 3: Managing Cybersecurity
Module 3 Tutorial: Understanding Digital Wellbeing and Ethics

In this tutorial activity, you will learn the importance of strong cybersecurity while handling data in the digital world.

Intended Learning Outcomes

Number	Description
ILO-1	Digital Wellbeing & Ethics: Understand and uphold ethical principles in using, applying, and developing digital and online tools.
ILO-2	Digital Wellbeing & Ethics: Practice responsible use of online platforms and appropriate online behavior.
ILO-3	Digital Wellbeing & Ethics: Recognize common online threats and apply appropriate methods to protect oneself online and be able to identify and respond appropriately to cybersecurity threats.

Lesson Overview

In this week's activity, students will learn the serious consequences of cyberattack and the need/importance of cybersecurity and the data ethics in place.

Activity 1: Data Security

Download the two datasets: COVID19CaseDetails and 3D-MazeDetails. Each group must answer the following questions,

a. According to the concepts of Data Security, discuss on the level of security you will provide to protect them.
b. As a student, discuss on the immediate actions you will take if this 3D maze data of yours gets breached.
c. As a hospital organization, discuss on the immediate actions you will take if this COVID details of your patients gets breached.
d. If you are required to send these two datasets through NTU email, what protection features you will use and why?

Activity 2: Role Playing Game

Scenario: Even though the NTU is known to have a strong cybersecurity in place, NTU's Human Resource (HR) office and Research Centers computers gets hacked by some hackers. Both the departments have informed of data breach due to this cyberattack.
Now each group will act as one of the characters and discuss on the concepts of cybersecurity and data security. Please note, your views should include the concepts of modules: cybersecurity covered in video learning modules. Prepare your answers to the questions asked in a word document/power point slides – for presentation later.

Group 1 & 2 – act as HR department and provide your view on the following questions.

a. Lists the consequences of this incident.
b. Discuss on the immediate actions to be taken by you after cyberattacking.
c. Discuss what could be done to prevent such attack in future.
d. How do you train your employee/staffs on this matter.

Group 3 & 4 – act as Research centers and provide your view on the following questions.

a. Lists the consequences of this incident.
b. Discuss on the immediate actions to be taken by you after cyberattacking.
c. Discuss what could be done to prevent such attack in future.
d. How do you train your employee/staffs on this matter.

Group 5 & 6 – act as NTU's cybersecurity team and provide your view on the following questions.

a. Discuss your immediate actions on this incident.
b. Lists the current measures in place to prevent cyberattack.
c. What do you think went wrong which led to this serious incident?
d. Discuss how you would prevent this incident from happening in future?
e. How do you train or provide awareness on this to all NTU staff and students?

Group 7 & 8 – act as NTU Management handling the Ethics and Compliance Committee and provide your view on the following questions.

a. Discuss your roles in this incident.
b. What measures you would take to minimize the damage due to this incident?
c. How would you handle the serious consequences (if reported) from this incident?
d. How do you provide awareness on this to all NTU staffs & students?

Group 9 & 10 –act as hackers and provide your view on the following questions.

a. Discuss on the methods you would have used to perform cyberattack.
b. Discuss on the difficulties faced and why in hacking the different types of data - having different levels of security?
c. Lists the possible ways you would misuse those hacked data.

Activity 3: Presentations

Presentations by instructor selected groups to show their answers to activities 1 & 2.

Roles of different departments/centers in NTU

1. NTU's Research Integrity and Ethics Office (RIEO)/Research Integrity Office (RIO)
    a. to provide key support required for researchers and other personnel in areas of research work involving humans and animals.
    b. also serves as the institutional representative to handle concerns raised by whistle-blowers involving allegations of research misconduct.
    c. provide support to successfully navigate the constantly evolving research environment.
    d. cases of possible research misconduct reported to the Ethics and Compliance Committee will be referred to the RIO.
    e. Visit https://www.ntu.edu.sg/research/research-integrity-office/research-integrity for more details.

2. Research Centers
    a. Please visit https://www.ntu.edu.sg/research/research-focus to know more about different research centers in NTU.
    b. Cyber Security Research Centre @ NTU (CYSREN) was established to address these concerns through multi-disciplinary research and development around cybersecurity, leveraging NTU's core competencies in Engineering, Exact Sciences, International Studies, and Business, among others. Visit https://www.ntu.edu.sg/cysren for more details.

3. Cybersecurity/Centre for IT Services (CITS) Teams
    a. To manage the campus-wide IT infrastructure and facilities of both staff and student.
    b. Manages the access to all Enterprise IT systems, as well as learning systems and digital media for both staff and student.
    c. Please visit https://www.ntu.edu.sg/life-at-ntu/internet-account-and-policy for more information.

Each group need to upload your work done on Module 3 tutorial in Discussion page of your tutorial site.

----------END OF TUTORIAL 4----------