UNIVERSITY OF MAKATI
J.P. Rizal Ext., West Rembo, Makati City

COLLEGE OF COMPUTING AND INFORMATION SCIENCES

Information Assurance and Security 2
Team Activity

Activity 2 : Need for Security

General Direction. Get a partner. Perform the following activities together. Discuss and answer the following questions. Only one member shall submit the final output in the TBL Hub.

I. Examine Data Breaches

The Privacy Rights Clearinghouse (PRC) is a nonprofit organization whose goals are to raise consumers' awareness of how technology affects personal privacy and empower consumers to take action to control their own personal information. The PRC maintains a searchable database of security breaches that impact consumer's privacy. In this project you will gather information from the PRC website.

1. Open a web browser and enter the URL **www.privacyrights.org/** data-breach.
The location of content on the Internet may change without warning. If you are no longer able to access the site through the above web address, use a search engine to search for "Privacy Rights Clearinghouse data breach".

2. First spend time reading about the PRC. Click About Us in the toolbar.

3. Scroll down to the content under Mission and Goals and also under Services. Spend a few minutes reading about the PRC.

4. Click your browser's Back button to return to the previous page.

5. On the Chronology of Data Breaches page scroll down and observe the different breaches listed in chronological order.

6. Now create a customized list of the data that will only list data breaches of educational institutions. Scroll back to the top of the page.

7. Under Select organization type(s), uncheck all organizations except EDU Educational Institutions.

8. Click GO!.

9. Scroll down to Breach Subtotal if necessary. How many breaches that were made public pertain to educational institutions?

10. Scroll down and observe the breaches for educational institutions.

11. Scroll back to the top of the page. Click New Search, located beneath the GO! button.

12. Now search for breaches that were a result of lost, discarded, or stolen equipment that belonged to the government and military. Under Choose the type of breaches to display, uncheck all types except Portable device (PORT) - Lost, discarded or stolen laptop, PDA, smartphone, portable memory device, CD, hard drive, data tape, etc.

13. Under Select organization type(s), uncheck all organizations except GOV – Government and Military.

14. Click GO!.

15. Scroll down to Breach Subtotal, if necessary. How many breaches that were made public pertain to this type?

16. Scroll down and observe the breaches for governmental institutions.

17. Scroll back to the top of the page.

18. Now create a search based on criteria that you are interested in, such as the Payment Card Fraud against Retail/Merchants during the current year.

19. When finished, close all windows.

QUESTIONS.

1. **Provide the screenshots as you perform the activity.**
2. **What are the important insights you learn from the output.**

II. Scan for Malware Using the Microsoft Safety Scanner

In this activity you will download and run the Microsoft Safety Scanner to determine if there is any malware on the computer.

1. Determine which system type of Windows you are running. Click **Start, Control Panel, System and Security**, and then **System**. Look under System type for the description.
2. Open your web browser and enter the URL **www.microsoft.com/security/scanner/en-us/default.asp**.

   The location of content on the Internet may change without warning. If you are no longer able to access the site through the above web address, use a search engine to search for "Microsoft Safety Scanner".

3. Click **Download Now**.
4. Select either **32-bit** or **64-bit**, depending upon which system type of Windows you are running.
5. When the program finishes downloading, right-click **Start** and click **Open Windows Explorer**.
6. Click the **Downloads** icon in the left pane.
7. Double-click the **msert.exe** file.
8. Click **Run**. If the **User Account Control** dialog box appears, click **Yes**.
9. Click the check box to accept the license terms for this software. Click **Next**.
10. Click **Next**.
11. Select **Quick scan** if necessary.
12. Click **Next**.

13. Depending on your computer this scan may take several minutes. Analyze the results of the scan to determine if there is any malicious software found in your computer.
14. If you have problems you can click **View detailed results of the scan**. After reviewing the results, click **OK**. If you do not find any problems, click **Finish**.
15. If any malicious software was found on your computer run the scan again and select **Full scan**. After the scan is complete, click **Finish** to close the dialog box.
16. Close all windows.

QUESTIONS.

1. **Provide the screenshots as you perform the activity.**
2. **Explain what is the output of your Full Scan.**
3. **Is this tool helpful to scan for Malware? Discuss your answer**

III. Research Cyber Kill Chain®

The Cyber Kill Chain approach to security is increasing in popularity. Research the background of the Cyber Kill Chain and how it is being used today. Begin by reading the original article "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains" by Eric M. Hutchins, Michael J. Clopperty, and Rohan M. Aminot at *www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf*. Next, search the Internet for additional information and how this approach can help improve security.

Due Date : 21 September 2023