Cyber Security

2024

Detect & Response

Vathna.lay@cadt.edu.kh

Scenarios

- Scenario 1: A student notices their laptop has become significantly slower, with frequent crashes and unexpected pop-ups. The battery also seems to drain faster than usual.
- Scenario2: A student receives an email that appears to be from their bank, warning of suspicious activity on their account and asking them to click a link to verify their information.
- Scenario 3: A student finds a new app on their smartphone that they don't remember downloading. The app is using a lot of data and seems to be running in the background constantly.
- Scenario 4: A student discovers a post on their social media account that they didn't create. The post contains a link to a suspicious website.

Scenarios

- Scenario 5: A student notices their webcam's LED light turning on intermittently, even when they are not using it.
- Scenario 6: A user types in the URL for their bank's website but is redirected to a different website with a similar-looking interface.The website prompts them for their login credentials.
- Scenario 7: A user notices a significant increase in their monthly data usage, even though their online activity hasn't changed. They haven't downloaded any large files or streamed videos excessively.

Scenarios

- Scenario 8: A user tries to log into their online banking account but finds their password no longer works. They try resetting their password, but the recovery email never arrives.
- Scenario 9: A user's printer suddenly starts printing documents they didn't initiate. The documents contain gibberish or strange symbols.
- Scenario 10: A user receives a pop-up message on their computer claiming that their system is infected with multiple viruses and urging them to click a button to download a "free antivirus" program.

Scenario 1: The Sluggish Laptop

- What are the possible causes of these issues?
- What steps should the we take to investigate and address the problem?
- Should they be concerned about a security breach? Why or why not?
- What additional information would be helpful in determining the cause?

Scenario 2: The Phishy Email

- What are the red flags in this email that might indicate a phishing attempt?
- How should we respond to this email?
- What could happen if the student clicks on the link?
- How can we protect themselves from similar attacks in the future?

Scenario 3: The Unexpected App

- What are the potential risks associated with this unknown app?
- What steps should we take to investigate the app and its behavior?
- Should we uninstall the app immediately? Why or why not?
- How can we prevent similar incidents from happening again?

Scenario 4: The Social Media Surprise

- What are the possible scenarios that could have led to this unauthorized post?
- What immediate steps should we take to protect their account and reputation?
- How can we determine if their account has been compromised?
- What steps should we take to secure our account and prevent future unauthorized access?

Scenario 5: The Webcam Woes

- What are the most likely reasons for this behavior?
- How can we determine if our webcam is being accessed without their knowledge?
- What steps should we take to secure our webcam and protect their privacy?
- What additional security measures could we implement to safeguard our devices and data?

Scenario 6: The Redirected Search

- What is likely happening in this scenario, and what type of attack could this be?
- What immediate steps should we take to protect ourselves?
- How can we verify if their DNS settings have been tampered with?
- Besides running a malware scan, what other actions can we take to mitigate the risk of future attacks?

Scenario 7: The Silent Data Thief

- What are the potential causes of this unexpected data usage, and which is the most concerning from a security perspective?
- How can we investigate the issue to determine the root cause?
- If malware is suspected, what steps should we take to mitigate the issue?
- How can we prevent similar issues in the future?

Scenario 8: The Locked-Out Account

- What are the most likely reasons for us being unable to access their account?
- What immediate actions should we take to address the situation?
- How can we determine if our account has been compromised?
- What steps can we take to prevent future account compromises?

Scenario 9: The Rogue Printer Job

- What are the potential explanations for this unexpected printer behavior?
- Why is it important to disconnect the printer from the network immediately?
- How can the user determine if a device on the network is compromised?
- What precautions can the user take to prevent future printer-related security incidents?

Scenario 10: The "Friendly" Warning

- Why is this pop-up message likely a scam?
- What actions should we take to protect their system?
- How can we avoid falling victim to similar scams in the future?
- If the pop-up persists, what further steps can we take?