جامعة الملك سعود
King Saud University
الإدارة العامة للأمن السيبراني

REPORT FOR A CYBER INCIDENT USER MANUAL

Terms

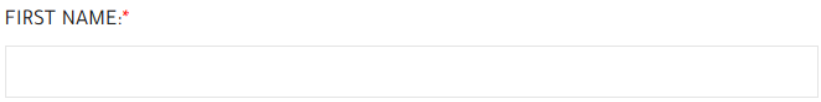
Term	Definition
Impact	The amount of damage or the consequence resulting from a vulnerability or security attack, such as service disruption or data loss.
Incident	Any unwanted or suspicious security event that may affect the confidentiality, integrity, or availability of information.
Phishing emails	Fraudulent messages often sent via email or social media aimed at tricking the user into providing sensitive information or installing malicious software.
Breach	Unauthorized access to a system, data, or network with the intent to modify, steal, or sabotage.
IP	Internet Protocol address, a unique number used to identify a device or server on a network.
Operating system	The core software that manages computers or phones and enables running applications, such as Windows, Linux, or Android.
Network	A group of interconnected devices that communicate with each other to exchange data, such as the Internet or local networks.
Data leak	The unauthorized disclosure of sensitive or confidential information, either accidentally or as the result of a cyberattack.
Website	A page or collection of pages on the Internet that can be accessed via a browser using a specific URL.
Vulnerability	A flaw or weakness in a system or application that can be exploited to carry out an attack or gain unauthorized access.
Ransomware	A type of malicious software that encrypts a victim's files and demands a financial ransom in exchange for the decryption key.

Guide Objectives

This guide aims to help users understand how to properly and effectively use the cyber incident reporting service by explaining the reporting steps and clarifying related technical terms. The guide ensures easy access to information and quick handling of any security report. It also contributes to raising security awareness and improving the quality of the service provided.

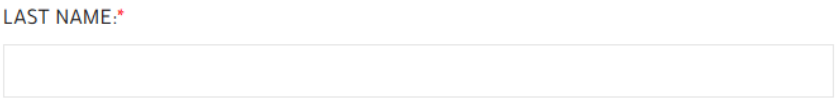
User Manual

1- First name



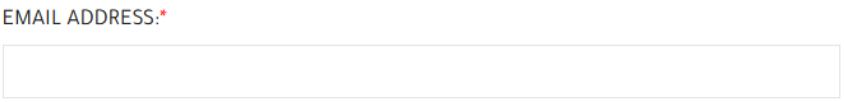
The sender's first name is recorded to facilitate communication and follow-up if needed.

2- Last name



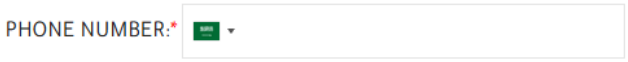
The sender's last name is recorded to facilitate communication and follow-up if needed.

3- Email Address



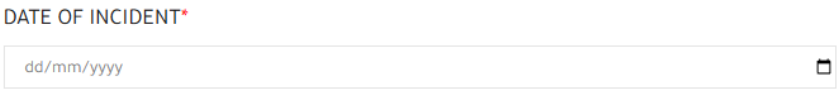
The sender's email address is recorded to facilitate communication and follow-up if needed.

4- Phone number



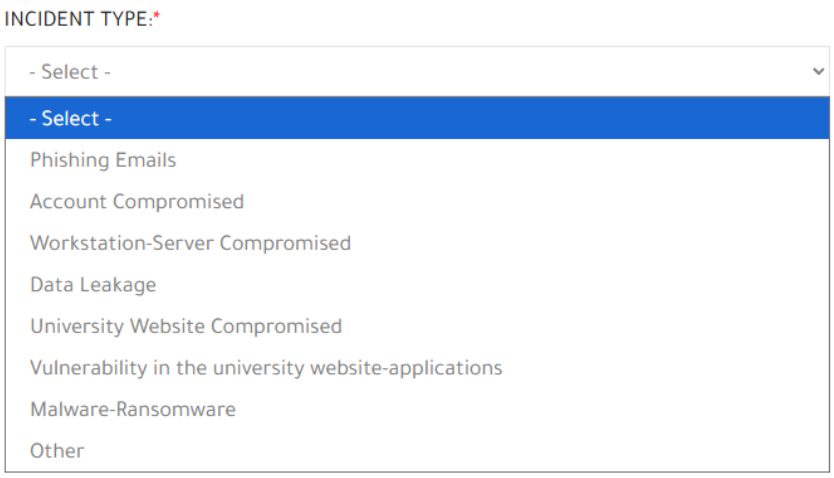
The sender's phone number is recorded to facilitate communication and follow-up if needed.

5- Date of incident



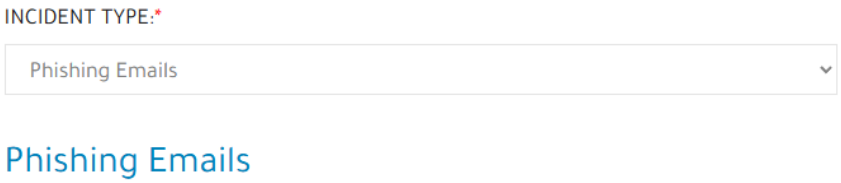
The date on which the incident occurred or was observed is specified.

6- Incident type

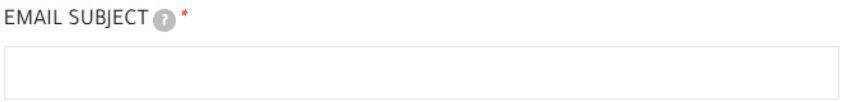


The type of incident that occurred on the university's systems, data, or services is selected.

a. Phishing emails

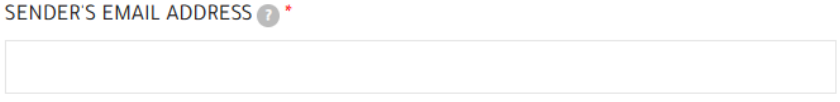


- Email subject



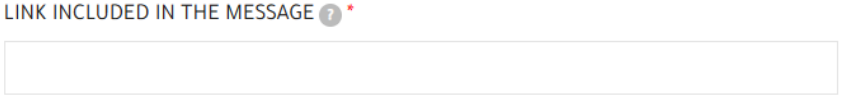
The subject line of the phishing message shown in the received email is recorded.

- Sender's email address



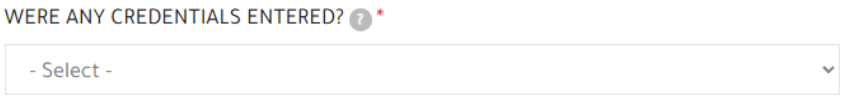
The sender's email address, as it appears in the phishing message, is recorded.

- Link included in the message



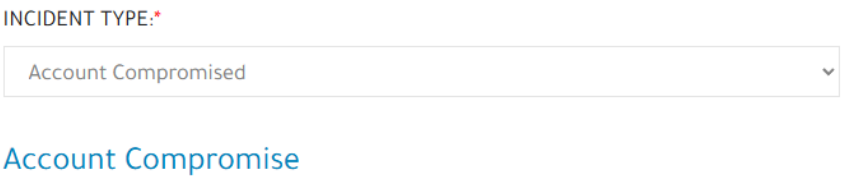
Paste the link attached in the phishing message, taking care **not** to visit/click the link.

- Where any credentials entered?

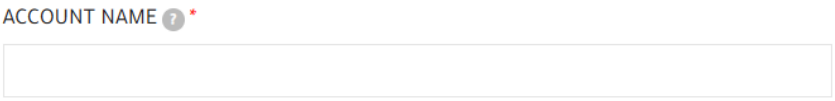


Answer "Yes" or "No" to indicate whether any information was entered into the link included in the phishing message.

b. Account compromise

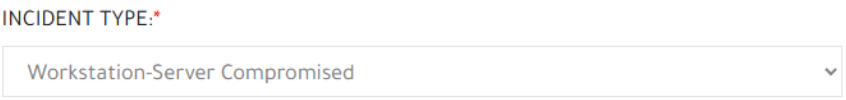


- Account name

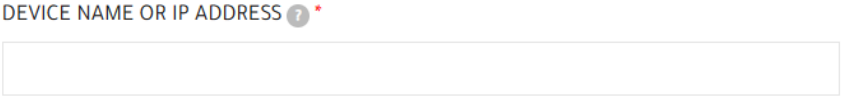


The name of the account or the email address that was compromised is recorded.

c. Workstation/server compromise

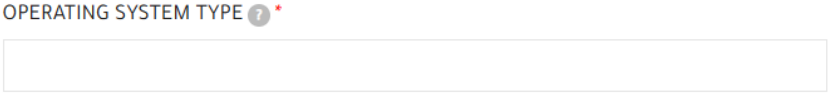


- Device name or IP address



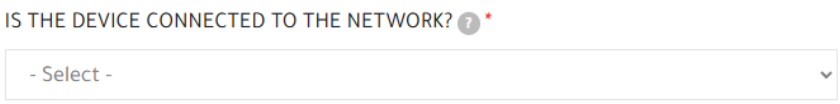
The name of the device or the IP address of the device or server that was compromised is recorded.

- Operating system type



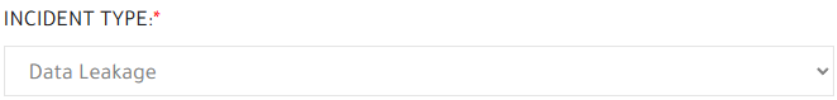
Specify the type of operating system used on the targeted device or server, including the version.

- Is the device connected to the network?



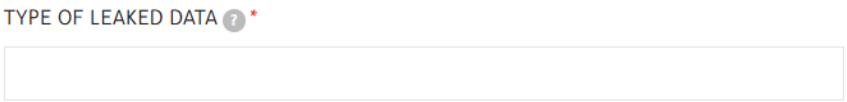
Indicate whether the device or server is still connected to the network or has been disconnected or shut down after the incident as a precautionary measure.

d. Data leakage



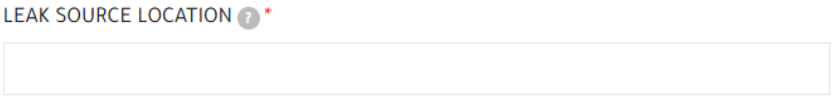
Data Leakage

- Type of leaked data



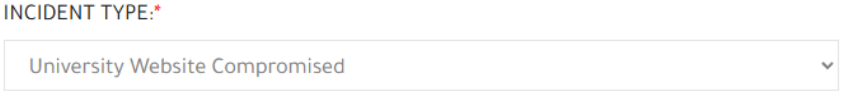
Specify the type of data that was leaked, such as personal data, financial data, or other sensitive information.

- Leak source location



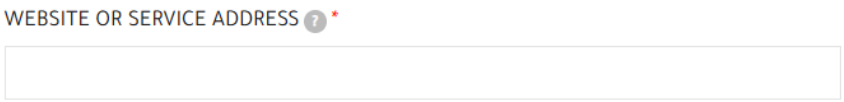
Specify the website or system where the data leak occurred, such as a website, database, or internal server.

e. University website compromise



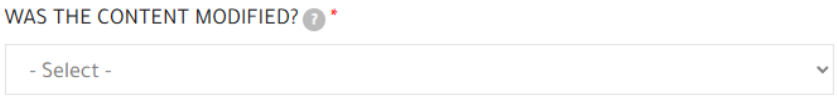
University Website Compromise

- Website or service address



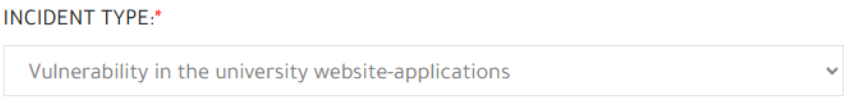
Enter the website address or the name of the service that was compromised to facilitate verification and remediation.

- Was the content modified?



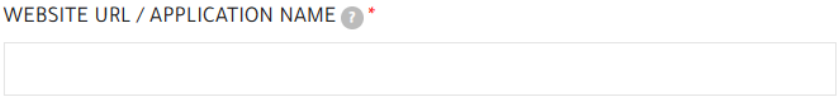
Please specify whether any modification or change in the content of the website or application was observed after the breach.

f. Vulnerability in the university website/application



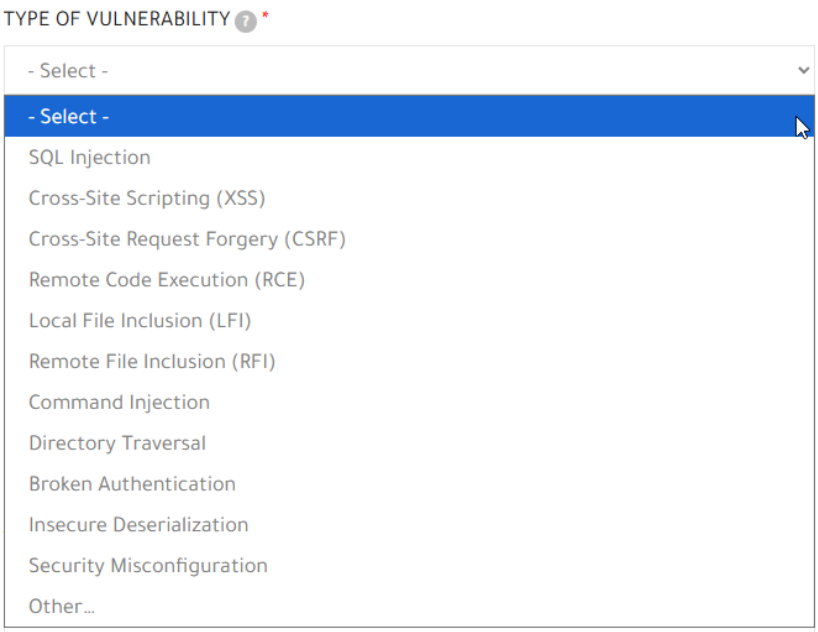
Vulnerability In The University Website/Applications

- Website URL / Application name



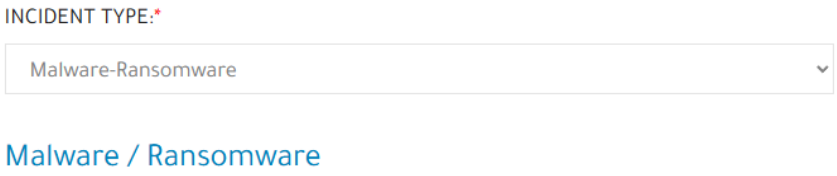
Enter the website address or the name of the service where the vulnerability was discovered to facilitate verification and remediation.

- Type of vulnerability



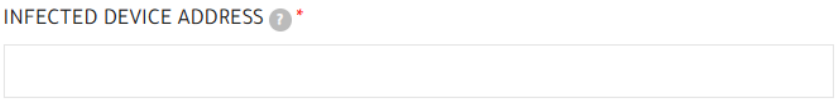
Select the type of security vulnerability from the list; if you choose "Other," please clearly write the name of the vulnerability in the designated field.

g. Malware / Ransomware



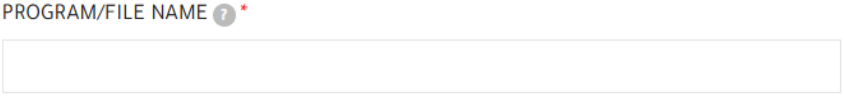
Malware / Ransomware

- Infected device address



Enter the IP address of the device infected with malware or ransomware.

- Program/file name

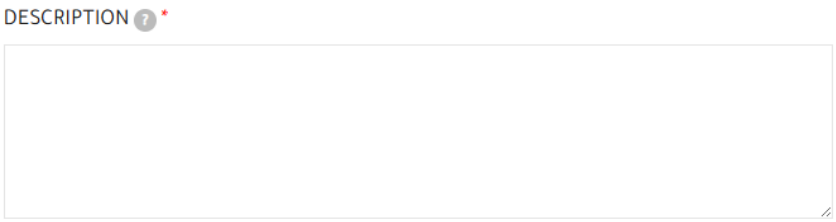


Enter the name of the malware or ransomware that was detected on the infected device.

7- Report Priority

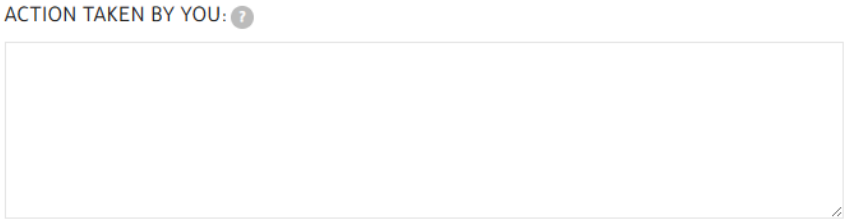
The report priority is selected to help ensure a prompt response and appropriate action.

8- Description



Please write a clear description of the incident, including what happened and the most notable impacts or changes observed on the systems or services.

9- Action taken by you



Please provide a detailed and clear explanation of all the measures taken to address the incident before submitting this report, to help facilitate effective follow-up.