

Nanyang Technological University
Center for IT Services
Security Incident Reporting Form



Instructions

Please try to fill in the form with as much information as possible. Some of the information is optional and/or not relevant; however, with as much information provided as possible, it enables CITS to provide you the best and fastest assistance.

For members of the public, we recommend that you approach your Internet Service Provider with the incident details.

Please return a **signed** copy of this form to NTU CITS through the internal mail system, via fax at +65 6791-0688 or at Centre for IT Services (NS4-02-21), Level 2, Academic Complex North, North Spine.

| | | | |
|---|--|---------------------|---|
| 1. Contact Information | | | |
| Please give us your contact information so that we may get back to you. | | | |
| Name | | Tel | |
| Email | | Handphone | |
| School/Dept. | | Are you a member of | Staff <input type="checkbox"/> Student <input type="checkbox"/> Public <input type="checkbox"/> |

| | | | |
|---|--------------------------|--------------------------|--------------------------|
| 2. Host Information | | | |
| Please give us as much information about your own computer system as possible. This will allow us to identify if there are any possible vulnerabilities that could be exploited in your system. | | | |
| Location of system | | | |
| Computer Name | | Operating System | |
| IP address | | MAC address | |
| For Windows systems, go to the command prompt, then run the command, "ipconfig /all" For other operating system, please refer to the user guide of the operating system. | | | |
| Did you install/enable the following? | Yes | No | Unknown |
| a. Latest security patches for your operating system | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| b. Anti-virus software (if yes, which one: _____) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| c. Latest anti-virus updates (if yes, which update: _____) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| d. Internet Relay Chat (IRC) Client | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| e. Messaging software (ICQ, Yahoo, MSN, etc.) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| f. Web server (IIS, Apache, etc) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| g. FTP server (IIS, Serv-U, WS_FTP server, etc.) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| h. SMTP server (IIS, QK SMTP, Postcast, etc. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| i. Terminal Services or Remote Desktop Connection enabled | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| j. Peer-to-peer file sharing software (Kazaa, Morpheus, eDonkey, etc) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| k. File and printer sharing | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| l. Personal firewall (if yes, which one: _____) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| m. Any other kind of server software? (Please indicate) | | | |

| | | | | | |
|---|--|------|--|------------------------------|-----------------------------|
| 3. Incident Information | | | | | |
| Please tell us as much as you can about the incident/s that you detected. This will allow us to provide you with the best response and resources. Please attach more sheets if there is insufficient space to record all the incidents. | | | | | |
| Incident No. | | Date | | Time | |
| What incident did you detect? | | | | | |
| How did you detect the incident? | | | | | |
| Do you have any log files of the incident? | | | | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| Please attach all log files if possible. You can either print out the logs, save the logs onto a diskette or cd-rom. | | | | | |
| Attacker's Computer Name | | | | Attacker's IP address | |
| Attacker's MAC address | | | | | |
| To get the attacker's details, run the following command, "nbtstat -a <Computer Name/IP address>," where <Computer Name/IP address> is the computer name or IP address of the attacker. NB: This will only work for Windows based machines on the NTU Network. | | | | | |
| Do you have any other information of the incident/attacker? | | | | | |
| | | | | | |

Declaration

I hereby declare that the information provided in this document is true to the best of my knowledge. I understand that the Centre for IT Services reserves the right to withhold the outcome of the investigation due to their legal liabilities and responsibilities as a registered Internet Service Provider.

Name:

Staff ID/Matric. No.:

Did you remember the following?

- Attach all log files
- Include your contact details
- Sign the declaration