A computer security incident is any attempted or successful unauthorized access, disclosure, or misuse of computing systems, data or networks, including hacking and theft.

#### scammer**REPORT A COMPUTER SECURITY INCIDENT**

Contact Information

* Email: helpdesk@lethbridgecollege.ca
* Phone: 403-320-3333
* Location: TE2208

**How to Report a Computer Security Incident:**

If you are not a system administrator and need to report a computer security incident, contact ITS helpdesk immediately.

If you are a system administrator, follow these steps to work with the Security Analyst to help:

* Manage security incidents at Lethbridge College
* Combat rising security and accountability risks
* Reduce associated costs

1. **Do not change the state of the machine you suspect has been compromised.**

* Do not turn off the machine.
* Do not remove the machine from the network unless active malicious agents are attempting to propagate or infect network resources.
* Do not look at the system to see what files are on it, or what might have been touched.

1. **Review security incident criteria.**

* A computer security incident is any attempted or successful unauthorized access, disclosure, or misuse of Lethbridge College computing systems, data or networks, including hacking and theft.
* Even if it’s just a suspicion that a Security event has occurred, it is better to report your suspicion rather than fail to prevent further damage from a valid suspicion.

1. **Contact the Lethbridge College helpdesk.**

* **The helpdesk will alert the Security Analyst of the incident.**

1. **Work with the Information Technology Security Analyst to:**

* Preserve and use forensic evidence to discover the extent of the intrusion
* Determine and minimize risk and the possibility of future risk to Lethbridge College
* Provide and maintain smooth and consistent interaction with law enforcement and Lethbridge College management

**Checklist for Lost or Stolen Mobile Devices**

* **Immediately report lost or stolen devices to the police** 
  + Always get an incident or report number
  + Call them back if item is found, including if a separate agency contacts you regarding a found device
* **If you used the device for work** 
  + Also report it to the ITS helpdesk so they can help identify and address potential compromised accounts or data
  + Notify your supervisor if it was a College-owned device
* For phones, notify your cellular carrier-- see if they can deactivate the device
* Change all passwords stored or used on the device, including email, Dropbox, banking, etc.
* Notify credit card companies and banks if you used the device for shopping or banking
* Try to track its location, if possible
* Try remote wipe if sensitive data or passwords were stored

**Reporting Spam and Phishing**

Spam and phishing complaints should be sent to the ITS helpdesk.