IT Security Incident Response Procedure

The IT Security Incident Response procedure helps to reduce the impact of a security incident by providing a consistent response.

Types of Incidents
IT security incidents may occur as a result of a variety of scenarios and for a variety of reasons but the primary result is to gain access to university resources. Some of the common types of IT security incidents experienced by the university occur as a result of accounts or devices being compromised in the following ways:

- **Phishing**: Sending fake emails that look like they are from the university (or other reputable businesses) that trick people into providing usernames and passwords.
- **Eavesdropping**: Spying on or intercepting digital communications that are insecure or installing devices that log keystrokes if they can get physical access to a device in order to obtain university account passwords.
- **Guessing**: Using software to manually trying to guess a password through a trial and error process.
- **Hijacking**: Taking over the electronic identity of a member from the university community to intercept or divert account and authentication information.
- **Stealing**: Stealing physical devices to extract or tamper with the account and password.
- **Malware**: Using malicious software such as viruses, worms, and spyware to cause intentional harm and to steal information.
- **Ransomware**: Using malicious software to encrypt data. Victims receive a message stating their files have been encrypted and demanding a ransom to have them decrypted.

How to Detect an Incident
Signs that you may be experiencing an IT security incident or have a compromised account include:

- Your username and password no longer work.
- Files or emails are being deleted.
- People tell you they are getting weird or unexpected emails from you.
- You get replies to emails you did not send.
- Software is being installed unexpectedly.
- Your anti-virus software has been disabled.
- Your device has unexpected popups appearing, runs very slowly, or crashes frequently.
- You cannot access system programs that you normally can access.

If you think you have experienced an IT security incident or have a compromised account, contact IT Support Services at:

- itsupport@usask.ca
- 306-966-2222
- 1-800-966-4817 (Toll Free in Canada)
The IT security incident response procedure is summarized in the four-steps below:

1. **Identification of IT Security Incident**
   IT security incidents are identified through both preventative and reactive measures. Any member of the university community should report to IT Support Services that it suspects or has confirmed that they have an IT security incident.

2. **Assessment of Impact of the IT Security Incident**
   Once an IT security incident is identified, IT Support Services and ICT Security assess the impact and scope of the incident to the university’s information, IT assets and IT systems to categorize the incident by severity.

   ![Assessment Factors for IT Security Incident Classification](image)

<table>
<thead>
<tr>
<th>Severity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRITICAL</td>
<td>Incidents that have significant consequences due to scope, scale, or volume of individuals impacted and that have severe or adverse effects on institutional operations, assets, or reputation.</td>
</tr>
<tr>
<td>HIGH</td>
<td>Incidents that result in direct financial impact or data loss or that may have severe or adverse effects on institutional operations, assets, or reputation.</td>
</tr>
<tr>
<td>MEDIUM</td>
<td>Incidents that do not have standard procedures, or that have standard procedures but the data that could be exposed or lost has higher risk. These incidents require additional investigation and analysis.</td>
</tr>
<tr>
<td>LOW</td>
<td>Incidents that have standard documented procedures and when the data that could be exposed or lost has lower risk.</td>
</tr>
</tbody>
</table>

3. **Response to the IT Security Incident**
   ICT will perform containment and eradication practices, such as disabling compromised accounts or systems, based on the severity of the IT security incident.

4. **Follow Up to IT Security Incident**
   The extent of follow up activities are dependent on the severity impact of the incident. This may include implementing enhanced account activity monitoring on an impacted accounts for a period of time, depending on the severity of the incident. In specific cases, additional security measures may be implemented.

To start the IT security incident response procedure, or if you have questions or comments, contact IT Support Services at:

- itsupport@usask.ca
- 306-966-2222
- 1-800-966-4817 (Toll Free in Canada)