

Reporting an IT Security Incident

In the event that you suspect that your laptop or account has been compromised, whether via a malicious actor, virus or malware. Please do as follows.

1. Do not shutdown your laptop.

Depending on the type of attack, shutting down your laptop can cause useful information to be lost if its a larger breach by a malicious actor. It's best that the laptop be left untouched so a security professional can investigate prior to taking action.

2. Call IT Support.

Please immediately call [IT Support](#) to report the issue so it can be investigated and escalated if necessary.

What happens afterwards?

If the incident is isolated to your laptop but further investigative work is required, you'll be provided with a spare to allow you to continue working in the meantime. For larger incidents you'll receive further instructions from IT Support or directly from the partners.

What Constitutes a IT Security Incident?

An IT Security Incident is any technology based attack which may compromise the confidentiality of our company or that of our clients. An IT Security Incident can include:

- Virus/malware infections.
- Keyloggers (records what you type on your keyboard).
- Data exfiltration whether via an external entity or an employee/contractor.
- Data breaches.
- Ransomware attacks (encrypts all data requiring payment to decrypt).

Revision #2

Created 13 October 2023 18:22:52 by Tyler Rasmussen

Updated 23 April 2024 22:16:20 by Tyler Rasmussen