Cyber Security Incident Reporting

OVERVIEW

Cyber Security threats are unfortunately commonplace, and although Universities are taking major steps to protect their users, systems and data, attacks are still successful and can be very disruption, so reporting incidents quickly can help stem an attack and protect University and user data and assets, leading to quicker recovery, less disruption, financial loss and reputational damage.

CONTACTS

Please Report All Cyber Security Incidents

https://mu.ie/supportportal

(01) 708 3830

servicedesk@mu.ie

(01) 708 3929 Campus Security (24hr line) campus.security@mu.ie

REPORTING

If you suspect an incident has occurred:

- Inform IT Services immediately, use the contact details above. Report even if the incident is on an external system. Provide as much information as possible on the nature of the incident, was it malware – something you downloaded, a data breach, or encryption related, what was the attack vector, e.g. a link in an email, how/when was the incident detected. IT Services will run the incident.
- Inform your line manager and colleagues – remember the incident may be quickly spreading to other devices on the network, or the phishing email could also be in their inbox.
- If your device is showing an encryption message from an attacker, or the device is unresponsive, do not attempt to use the device, remove the device from the network if possible, if you cannot do this, shut it down, but do not reboot the device as this may increase overall damage.
- Do not consider contacting the attacker, or paying a ransom.

RESPONDING TO AN INCIDENT WITHIN YOUR AREA

- Assemble (physically/virtually) your previously identified core team to manage the response for your area – alternative means of communication may be required to achieve this, as University IT may not be usable.
- Enact your Business Continuity Plan.
- Review and clear communications with Marketing and Communications before contacting Staff, Students and External Bodies. This is extremely important as all incident communications need to have official clearance.
- Remember IT Services will be responding to mitigate the incident and the University Major Incident Team may also be activated and information on the availability of University facilities, including technology, for teaching, research and administration will be issued by these areas and will need to be acted on.

CYBER SECURITY IS EVERYONE'S RESPONSIBILITY