

# Cyber Security Guidance




## OVERVIEW

Cyber Security Awareness and Preparedness are of the utmost importance to the Higher Education sector as it continues to be targeted by cyber criminals.

IT Services have controls in place to monitor and mitigate attacks, but all University users have a responsibility to help protect our data and systems by being alert to the dangers and by following best practice.

## BE AWARE – BE READY

- Make sure you and your staff are cyber security aware and are trained.
- Know the technologies your area operates and the associated cyber security risks and mitigate those risks. Don't be afraid to ask for IT Services help.
- Pre-plan for an incident, know:
  - Who would be the core team needed to deal with the incident.
  - How to and what to communicate with your key staff/teams and your students.
- Review and test your Business Continuity Plan.
- Be very cautious using public/unsecured Wi-Fi, it can be used to distribute malware and steal data.
- When entering information online only use secured sites that you trust, look out for the  (*padlock*) or *https://* in the browser link.
- Look out for Phishing emails/websites and generally think twice before clicking links in emails and documents. Report Phishing emails to IT Services.

## CONTACTS

Please Report All Cyber Security Incidents



<https://mu.ie/supportportal>




(01) 708 3830



[servicedesk@mu.ie](mailto:servicedesk@mu.ie)



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

## DO

- Keep your device operating system, Apps and software up to date.
- Always use multi-factor authentication.
- Back up important files frequently, e.g. using the Microsoft 365 tools.
- Be careful what you share on social media, it could be used to target you.
- Review IT related security policies regularly.

## DO NOT

- Do not share your usernames and passwords with anyone.
- Do not use the same password for all your Systems and Apps.
- Do not download external Apps or Programs to your University devices that are not sanctioned.

**CYBER SECURITY IS EVERYONE'S RESPONSIBILITY**