Related to viruses, the UM Information Confidentiality/Security Policy states:

- University owned computers and servers must have software installed to protect against viruses from the Internet or other machines. The software should be configured to perform daily update checks, preferably in an active or real time scan mode.

- Contact the IT Helpdesk for information on campus-wide site licensing for anti-virus software.

- When a virus is detected, immediately disconnect the infected machine(s) from all networks and contact your systems administrator.

- In cases in which a systems administrator manages multiple machines, he/she should contact all users with access to the infected system, explain how to determine if related systems are infected, and how to remove the virus.

- See the Anti-Virus Protection for UM Computers Policy for additional information.
Employee Termination Process

The University’s Employee Exit Checklist must be used consistently within departments.

- The Employee Exit Checklist must be completed anytime an employee terminates from the University or transfers departments within the University.
- The checklist can be accessed through the Human Resources website.
- Completed checklists must be forwarded to Human Resources.
- A non-mandatory Student Exit Checklist is also available on the Human Resources website for departmental use. These should not be forwarded to Human Resources.
- Checklists help ensure that all appropriate actions are taken in a timely manner in the event of employee turnover.

Reminder

Care should be exercised when clicking on links & attachments from unknown sources. Remember, IT will never ask for user names and passwords via email.