جامعة الحمدانية /كلية التربية

قسم علوم الحاسوب

Fourth Class

Data Security

أستاذ المادة:

م. سماح فخري عزيز

- **Steps to Better Security2**

CONTENTS

- Steps to Better Security
  - Encrypt all devices
  - Delete redundant data
  - Update your programs regularly
  - Back-up your data regularly
  - Establish strong passwords
- Steps to Better Security
  - Use Network Drives for Sensitive or Important Files
  - Do Not Let Another Person Use Your User Account
  - Malware prevention
  - User education and awareness
  - Review your privacy settings

- **Encrypt all devices**

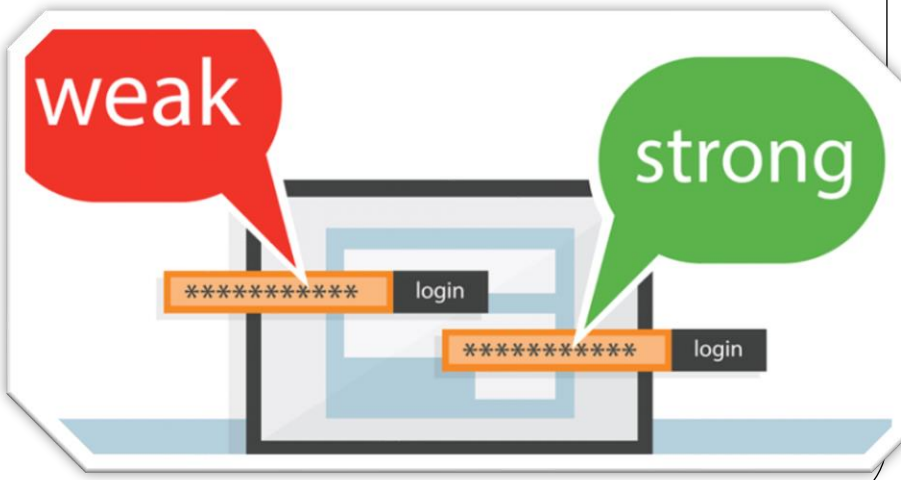
- *Make sure that all data is stored in an encrypted format and remains encrypted during migrations.*

- **Delete redundant data**

- *Ensuring information disposal mechanisms are in place helps prevent stale data from being forgotten about and stolen at a later date.*

- **Establish strong passwords**
- *Implementing strong passwords is the first step you can take to strengthen your security in this area.*

- *Use reasonably complex passwords and change them at least every 90 days.*



- **Back-up your data regularly**

- *backup data should be stored in a secure, remote location away from your primary place of business.*

- **Update your programs regularly**

- ***Make sure your computer is properly patched and updated. This is often the best way to ensure its adequately protected.***

- **Use Network Drives for Sensitive or Important Files**

- *All files that contain sensitive information, or that are critical to the work should be stored on a network drive – but only as long as they are needed.*

- **Do Not Let Another Person Use Your User Account**

- *Your user account represents all the computing resources that you personally have been authorized to access.*

- *By letting someone else use your user account, you are letting them access resources for which they may not have approval. Anything that they may do will, ultimately, be your responsibility.*

Malware prevention

- *There are many ways malware can infect an organization's systems. It could be sent in an email attachment, worm through a vulnerability or be plugged into an office computer via a removable device.*

- *To mitigate these risks, organizations should implement anti-malware software and policies designed to help prevent employees from falling victim.*

- **User education and awareness**

- *Employees play an essential role in their organization's security practices, so they need to be taught their responsibilities and shown what they can do to prevent data breaches.*

- *Training can come in many forms, from introductory e-learning to classroom-based certification courses. It's up to you to decide which level of training is appropriate for your employees.*

- **Review your privacy settings**

- *Review the settings on social networks and sharing sites to make sure your are sharing your data with whom you intend to.*

Thank you