Medical Sciences Division IT

Password Creation Guidelines

Passwords are used for various purposes at the University. Some of the more common uses include: user-level accounts, web accounts, email accounts and screen saver protection. The best practice suggestions for password creation and protection are summarized below.

Strong passwords have the following characteristics:

- They contains a mixture of both upper and lower case characters (i.e., a-z, A-Z)
- They have digits and punctuation characters as well as letters: i.e., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- They are at least fifteen alphanumeric characters long
- They are not a word in any language, slang, dialect, jargon, etc. Unusual combinations of words might offer good protection
- They are not based on personal information, names of family, names of pets, phone numbers, car registration number, etc.
- They are never written down or stored on-line. Try to create passwords that can be easily remembered
- One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.
  Please do not use these examples !

Password Protection Standards

- Do not use the same password for University accounts as for other non-University access (e.g. personal ISP account, banking services, benefits, etc.). Where possible, don't use the same password for various University access needs. For example, select one password for the Nexus email system and a separate password for MSD IT systems
- Don't reveal a password to ANYONE in person or over the phone
- Don't reveal a password in an email message
- Don't reveal a password to a manager, an IT support officer, or a colleague before going on holiday

- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- If someone demands your password, refer them to this document or have them call the MSD IT Help desk
- Do not use the "Remember Password" feature of applications (e.g., Eudora, Outlook, Thunderbird, Mac Mail, etc.)
- Do not write passwords down and do not store them anywhere in your office. Do not store passwords in a file on ANY computer system (including smart phones, tablets, or similar devices) without encryption
- Although the MSD IT Policy enforces a password change every 12 month, it can be good to change passwords more frequently
- If an account or password is suspected to have been compromised, report the incident to MSD IT and change all passwords