Network Password Guidelines

Information Services

Passwords are an important aspect of computer security and the failure to use strong passwords may lead to the compromise of information and information systems. This document provides useful guidelines on how to construct and use passwords to keep information safe.

1. Constructing strong passwords

Passwords should always have a meaning i.e. they should be difficult to guess but easy to remember, and as they are valuable they should always be kept safe, so please don't share them or leave them where they can be seen and discovered.

When choosing passwords, to meet the length and complexity rules you could try using the following methods:

- use the first letter of each word in a memorable phrase, saying, nursery rhyme or song title e.g. "Do you know the way to San Jose" becomes dyKtw2SJ?
- use an ordinary word or phrase and change, delete or add characters so that it becomes nonsensical e.g. Cranfield = £r@n5ielD
- try typing entire pass-phrases, such as "Wonderful weather today" but substituting some letters with numbers and special characters e.g. "Wond3rfulwe@thertoday?"

2. Remember – Keep your information safe

Access to on-line information is becoming increasingly important and all users have a responsibility to protect themselves and the value of information entrusted to them. You can imagine how embarrassing it would be if somebody accessed your account and send derogatory emails to your line manager/lecturer! Always remember that your password provides access to a range of University services including your valuable personal data so protect it and your on-line identity accordingly.

Never let other users see you type your password into systems – known as shoulder surfing – and always avoid using common 'dictionary' words (attackers' will target these to try and find a match) or any easily discoverable information like the name of a favourite sports team, pet, etc.

If you suspect that your account has been compromised, or abused, or is always 'locked' out when you want to use it please notify the IT Service Desk, and if you believe your password has become known or been compromised then change it immediately.

Please ensure that you set an appropriate password/PIN (or similar biometric security feature) on any device that is used to access University data.

You can change your password on a campus Windows PC by using Ctrl+Alt+Del, or by using Password Manager, which is available on the internet at: www.cranfield.ac.uk/pwman

Document control

Document title	Network Password Guidelines
Document number	CU-IT-PROC-9.01
Originator name/document owner	Information Security
Professional Service Unit/Department	Information Services
Approval by and date	Information Assurance Committee; 28/09/2020
Date of last review and version number	September 2020; V1.5
Date of next review	August 2021
Information categorisation	Open

Document Review

Version	Amendment	By	Date
1.4	Date changes only	Information Security	September 2019
1.5	Date and numbering amendments	Information Security	September 2020