a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD #02
Password and Passphrase Protection

Introduction

1. This document defines standards for the creation and use of passwords and passphrases to protect the UBC Electronic Information that Users handle.
2. Passwords (words or strings of characters) and passphrases (sequences of words or other text) are common and important ways to access and protect digital information on or off the Internet through almost any type of device. Consequently, attackers attempting to access information use a variety of tools to guess or steal passwords/passphrases.
3. In summary, the top three ways to keep a password/passphrase safe and protect the information are:
   a. create a strong password/passphrase;
   b. guard it carefully (e.g. don't share it or write it down); and
   c. avoid reusing it for other systems.
4. The Chief Information Officer has issued this document under the authority of Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

Creating a Password/Passphrase

5. Passwords must contain a minimum of 8 characters including upper and lower case letters, numbers and symbols. Alternatively, use a passphrase with a minimum of 16 characters. Guidelines for consideration:
   a. To create a complex short password, consider using the first letter of each word in a phrase. For example, "I ride my bike to school at 7 AM!" becomes "Irmbtsa7AM!".
   b. To create a passphrase, consider using a sentence or part of a sentence, or a phrase of disconnected words (e.g. "plug in sunshine thimbles" or "stingers sing paint").
   c. Avoid using a password/passphrase that replaces a letter with a number, such as "Br0adcast!" where the "O" is replaced with a zero. Password guessing programs can easily crack these.
   d. Password generation and storage programs should be used to create and manage passwords/passphrases.
   e. Name, username, address, or date of birth should not be used to create a password/passphrase. These items are too easily guessed by attackers. Also, any term that can be guessed by someone that Users know well should not be used.

Bad (Easy to Guess)	Good (Hard to Guess)
password	Pass turtle phrase
123456	the sky sings gold
12345678	One plus two beach
abc123	ABC is not like 123
qwerty	Quietly walks trees.
monkey	Monkey Pats Dog
dragon	Dragon singes cat!
111111	1 pickle flies badly
letmein	let me cloud in

Changing a Password/Passphrase

6. Passwords/passphrases for all university user accounts must be changed annually. When changing a password/passphrase:
   a. do not use the 10 most recent passwords/passphrases that have been used on the same system;
   b. do not use the same passwords/passphrases for personal accounts and university accounts; and
   c. it is recommended to use unique passwords/passphrases for different accounts, so that even if one is stolen, it does not allow access to other accounts owned by the same User; however, it is acceptable to use the same password/passphrase across university accounts.

Protecting a Password/Passphrase

7. If a password/passphrase is written down, it must be locked away in a secure, inaccessible location such as a safe.
8. Best practices state that passwords should not be shared for any reason - even with trusted individuals such as supervisors.
9. University IT Support Staff will never ask for Users' passwords.
10. Do not respond to Emails or phone calls requesting passwords/passphrases, even if they appear to be from a trusted source. These requests are often attempts to steal Users' credentials.
11. Passwords/passphrases must be immediately changed if there are suspicions that they could have been compromised and the incident must be reported to UBC Information Security (see the Reporting Information Security Incidents standard).
12. If a password safe (an application for securely storing multiple passwords) is to be used, refer to the Password Safe guideline.

Case Study: Why You Shouldn't Share Your Password

A single user ID and password was shared amongst a research lab's personnel. One of these individuals maliciously destroyed some of the data in the account. Since this was a shared account, it was challenging to identify the responsible party.

Passwords/Passphrases for Mobile Devices

13. Laptops and Mobile Computing Devices must be configured with passwords. Due to Mobile Computing Devices (smartphones and tablets) having touch-screen interfaces, it is not practical to use a strong password to lock the device. Instead, a password/PIN lock that is at least 5 characters long can be used.
14. See the Securing Computing and Mobile Storage Devices/Media standard for further requirements regarding mobile device security.

Choosing your PIN

A simple PIN option is to think of a 5 or 6 letter word and spell it out using the letters on the numeric key pad. Example: HOUSE becomes "46873".

Additional Requirements for University IT Support Staff

15. For University IT Support Staff, there are additional requirements around the storage of passwords/passphrases. These requirements are detailed in the User Account Management standard.

Related Documents

Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems

Securing Computing and Mobile Storage Devices/Media standard

Reporting Information Security Incidents standard

User Account Management standard

Password Safe guideline