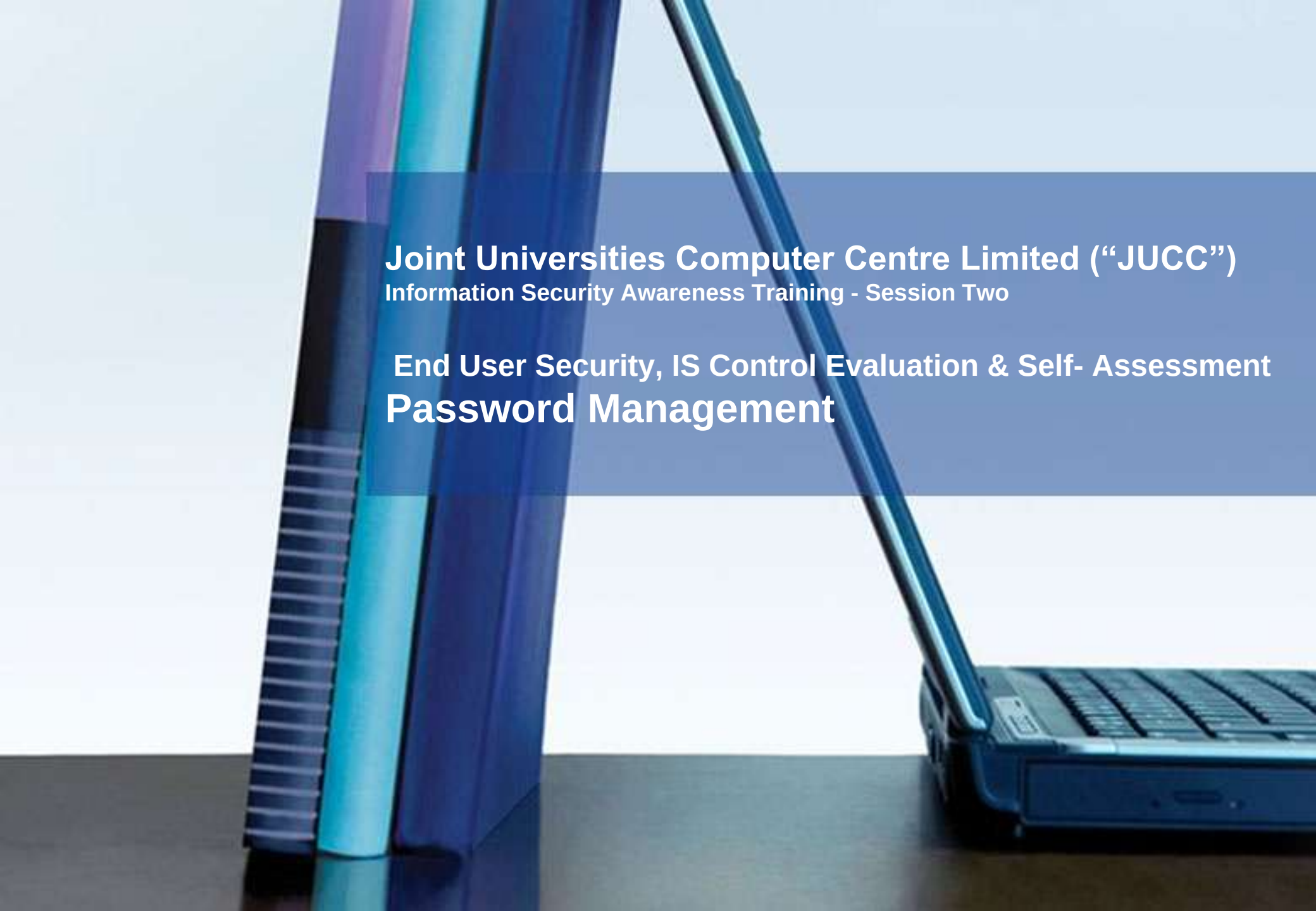

Joint Universities Computer Centre Limited (“JUCC”)

Information Security Awareness Training - Session Two

End User Security, IS Control Evaluation & Self- Assessment

Password Management

Agenda

- Password Fundamentals
  - Defining Password
  - Password Cracking in the Real World
- Strong Password
  - What is a Strong Password
  - Password components
  - Passphrase
- Password Management
  - Password Management Tools and Tactics
  - Password Management Best Practices

Defining Password

A password is a secret word or string of characters that is used for authentication, to prove identity or gain access to a resource

Identification and authentication

- User identifier – username ➔ **To distinguish**
- Authentication – password ➔ **To prove**

Password Cracking

- Password cracking is the process of **recovering passwords from data** that has been stored in or transmitted by a computer system
- Cracking involves attempting to **discover a character string that will produce the same encrypted hash as the target password**

Common Password Cracking Techniques

- **Dictionary attack**

Attack/ hack user passwords according to a list of dictionary words

- **Brute force attack**

Running a password cracking program through all combinations of letters, symbols and numbers until it gets a match with the target password

- **Hybrid attack**

Adding numbers or symbols to dictionary words when cracking user passwords

Password Cracking in the Real World

Issue: Mac's vulnerability in password system

- Users' password on Mac OS x Lion may be extracted by passware when the computer is locked or resided in sleep modes

Process time

- The process takes a few minutes, regardless of password strength and use of a FileVault encryption

Security tips

- Disable automatic login
- Disable FireWire port

Password Cracking in the Real World

Issue: Advanced WinXP Password Cracking

- New technology allows fast cracking of WinXP password hash up to 14 characters with special characters

Process time

- For 14 characters password, within 5.3 seconds

Security tips

- Secure the machines physically
- Consider using passphrase with more than 14 characters

Strong Password

What is a Strong Password?

- Desirably long and complex
- Unpredictable of its character
- Mitigate guessing and cracking

Common Password Pitfalls

- Dictionary words in any language
- Words spelled backwards, common misspellings, and abbreviations
- Sequences or repeated characters (eg: 12345678, 222222, abcdefg, or adjacent letters on the keyboard (qwerty)
- Personal information (eg: Name, birthday, driver's license, passport number, etc.)

Your Password should…

1. Length

- Be at least 8-character long

2. Complexity

Contain a mix of:

- Uppercase letters (A-Z)
- Lowercase letters (a-z)
- Digits (0-9)
- Symbols

Your Password should…

3. Password History

- Not be reused, at least for your past 5-10 passwords
- Advanced password history avoid simple incremental changes

4. Expiry

- Be changed at least every 90 days

5. Account Lockout

- Your account will be disabled or suspended after a certain number of incorrect log-in attempts

Your Password should…

A Video Example

http://www.youtube.com/watch?v=COU5T-Wafa4

Passphrase

What is a passphrase?

- A sequence of words or text used to control access to a computer system, program or data
- *Example: weboftrustisbrokencanyouglueitbacktogether?*

  (Web of trust is broken, can you glue it back together?)

Length

- Generally longer than password – 20 to 30 characters

Typical usage

- Controls both access to, and operation of, cryptographic programs and systems
- Provides additional security
- Serves as an encryption key

Passphrase

Characteristics of a good passphrase

- Sufficiently long to avoid guessing
- Use of symbol substitution (e.g.: substituting an “a” with “@”)
- Not a famous quotation from literature

Example steps

- Start with a normal phrase
- Randomly distort it (e.g.: switching the sentence structure)
- Add a few random words or characters to enhance security

Example

- isetmyp@ssw0rdright!

Password Management Tools

1. **Single sign-on (“SSO”) technology**
   User is required to be authenticated once to gain access to all authorised information and resources.

2. **Password synchronisation**
   User is only required to use one password to gain access to all authorised resources. The same password is automatically synchronised among systems within the same trusted environment upon changes.

Password Management Tactics

1. Use of local password management software

- User is required to use only one master password to gain access to a list of usernames, passwords and other information of different systems.
- Dedicated password management software or securely protected spreadsheets can be utilised.

2. Use of password generation tools

- Password is generated by combining a password prefix with the name of the application/ website.
- E.g.: “mypassword” + “gmail” mGyMp@@sIsLw0rd
- Inputting the password prefix and application name to the tool retrieves the same password each time.

3. Use of password tiers

For each password tier, a password is created for a group of applications with similar security level.

Example of password tiers

Tier 1	• Applications requiring the highest security level (e.g.: online banking, electronic payment and government websites) • Password: myvEry1^^port@ntpw!
Tier 2	• Applications requiring medium security level (e.g. : service providers' web portals) • Password: m3d!uM414!
Tier 3	• Applications requiring a lower security level (e.g.: public forums, social-networking websites and online subscription) • Password: s0meP@ssword

Password Management Best Practices

Do's

- Change password on a regular basis
- Change temporary or default passwords at the first log-in
- Test password strength before use with reliable 'Password Check' tools

Don'ts

- Do not keep unsecured records of password (e.g.: writing password on post-it)
- Do not use the same password between sites, applications and other different sources
- Do not use double words (e.g.: "hellohello")
- Do not use commonly known identifiers in password (e.g.: username, phone number or date of birth)
- Do not use dictionary words or famous quotes as password
- Do not use common sequences from a keyboard row as password (e.g.: "qwerty")

Password Management Best Practices

Online Password Check:

- http://www.microsoft.com/canada/athome/security/privacy/password_checker.mspx

Password Generator:

- http://strongpasswordgenerator.com/
- http://ss64.com/passwords/

Summary

- Password management should be educated and promoted campus-wide. It requires commitment of both the university and general users to enforce a highly secured environment
- Password management practices should be assessed and tested periodically to ensure safety amidst increasing number of intruders and hacking activities

Q&A

?

Copyright Statement