Course Title	:	Personal Security in Cyberspace
Course Code	:	CLD9006/GED122/CDS122
No. of Credits/Term	:	3
Mode of Tuition	:	Sectional Approach
Class Contact Hours	:	3 hours per week
Category in Major Prog.	:	Science, Technology and Society Cluster Course/ General Education Category D/Free Elective
Prerequisites	:	Nil

Brief Course Description

This course examines the misunderstanding of security from user behaviour perspectives. Many users believe their connections in cyberspace are safe and they do not realize the serious consequences of possible security breaches. This course shows the various threats in cyberspace. Consequences of security breaches will be discussed. It will also cover countermeasures which can protect cyberspace users. It provides a foundation for students to understand the technology which they use every day. Students will be able to protect themselves in cyberspace on completion of this course.

Aims

To introduce security methods which can protect students in Cyberspace.

Learning Outcomes

On Completion of this course, students should be able to:

1. Identify and describe the threats in cyberspace
2. Identify the consequences of security breaches, and compare and contrast the threat levels and the impact on the hosted data.
3. Evaluate the strengths, weakness, costs and benefits of different types of countermeasures
4. Select the best countermeasures to protect themselves in different situations, and describe the strengths and weaknesses of different potential countermeasures.
5. Implement the selected countermeasures and review their effectiveness

As the above outcomes are closely related to each other, students should achieve all outcomes in order to get the maximum benefits from taking this course.

Measurement of Learning Outcomes

1. Experiments will be conducted in computer room and students' performance will be assessed. These will test students' abilities to implement countermeasures and review their effectiveness.
2. Classroom activities will assess students' abilities to identify security threats, evaluate and select countermeasures.

3. Group projects will test students' abilities to analyse threats, develop and select effective countermeasures of complex cases in cyberspace. Students' presentation skills will also be assessed.
4. Final examination will be used to assess the students' comprehension of the concepts of topics which have been taught in the course.

Indicative Contents

IT Security

1. Latest Technologies in Cyberspace and their Vulnerabilities
2. Basic Concepts in Computer Security
3. Encryption and Related Techniques
4. Methods for Threats Identification
5. Countermeasures
6. Continuity and Disaster Recovery Plan
7. Ethical Conducts in Cyberspace

Threats in Cyberspace

1. Eavesdropping
2. Stealing Bandwidth
3. Man-in-the-Middle (MITM) attack
4. Bogus Access Point
5. Bogus Web Server
6. Unauthorized Connections
7. "Social Engineering" Techniques

Electronic Payment

1. Barriers to Cashless Society
2. Digital Cash and Impact
3. Electronic Credit Card
4. Electronic Fund Transfer
5. Electronic Cheque
6. Micropayment

Digital Certificate

1. Certificate Authority (CA) and related legal issues
2. Public Key Infrastructures
3. Digital Signatures
4. Configuration of Internet Browsers and Mail Clients
5. "Two Factor" Authentication
6. Renew and revoke Certificate
7. Web Server with Secure Socket Layer (SSL)
8. Comparison with Virtual Public Network (VPN) and other technologies
9. Green Computing

Teaching Method

Materials will be taught through lecturing, project assignments, presentations, discussion and demonstration in laboratory. Students will be asked to demonstrate their understanding of the subject through presentation and/or assignment.

Assessment

Students are expected to participate actively in experiments and discussions of case studies in classes. Their performance will be used to assess their abilities to identify the threats and implement countermeasures effectively. Group projects will be used to assess the students' abilities to handle complex cases. Test and examination will be used to assess the students' overall comprehension of the course.

Attendance and Participation	10%
Mid-term Test	10%
Project	30%
Final Exam	50%
Total	100%

Course Website

Course materials (projects, presentation slides) and information related to the course will be maintained on the website. Students can access this website through the WebCT. Students are advised to check on this website frequently.

Required/Essential Readings

Chuch Easttom, *Computer Security Fundamental*, Pearson, 2nd ed.,

Recommended/Supplementary Readings

Smith, A., *Internet retail banking: A competitive analysis in an increasingly financially troubled environment, Information Management & Computer Security*, Vol. 17, Number 2, pp. 127-150, 2009.

Berghel H., *Phishing Mongers and Posers*, Communications of the ACM, v49, n4, 2006.