BIRZEIT UNIVERSITY

Faculty of Engineering and Technology

Department of Computer Science

Usable Security and Privacy

Course Outline – 1st Semester 2024/2025

Overview:

This course will discuss one of the most challenging problems in computer security; the human factor. User errors are the most common cause of security failures, yet most security systems overlook usability design. Historically, human factors and usability have played only a limited role in security research and secure systems development. Security experts have neglected usability issues because they don't recognize the importance of human factors and their lack of expertise to address them.

Course Goals:

- Gain a better understanding of the relevance of usability in the context of security and privacy.
- Identify privacy and security concerns related to usability and user interface.
- Develop the ability to design studies to evaluate usability issues in security and privacy technologies.

Prerequisites:

- COMP231 (Advanced Programming)

Instructor: Dr. Abdallah Karakra

Course Materials:

- Required Textbook: Security and Usability: Designing Secure Systems that People Can Use by Lorrie Faith Cranor and Simson Garfinkel, O'Reilly, 2005
- Other references
  - Usable Security History, Themes, and Challenges by Simson Garfinkel and Heather Richter Lipford, Morgan & Claypool ,2014
  - Research papers provided by the instructor
  - Online Resources and Lecture Notes

Methods of Instruction:

- Lectures, case studies, and reading papers.

Student Evaluation: **(Tentative: this might change according to the teaching situation)**

- Quizzes 10%
- Midterm exam 30%
- Assignments 10%
- Project 15%
- Final exam 35

Course Outline:

#	Description	# of Lectures
1	Overview of Usable Security and Privacy	1
2	Introduction to Security, Case Study: SSL Warning	4
Assignment 1		
3	Introduction to Privacy, Case Study: Privacy Policy	3
4	Fundamentals of Human-Computer Interaction, Case Studies: Banking App Security, Social Media Privacy Settings	3
Assignment 2 & Phase 1 Project		
5	Psychological Acceptability Revisited, Case Studies: The Memorability and Security of Passwords, Existing Advice on Password Selection, Graphical Passwords	5
Midterm Exam (30%)		
Phase 2 Project		
6	Usability, Tasks, Chunking Information, Mental Models	2
7	Usability Design, Design Methodology, Case Study: Usability Involvement in a Security Application	3
Assignment 3		
8	Usability Studies, A/B Testing, Quantitative and Qualitative Evaluation, Case Study: Phishing Email	2
9	Authentication Mechanisms, Biometrics, Two-Factor Authentication	2
10	Authority, Guidelines for Interface Design, Case Study: Phishing Warnings	3
11	Privacy Settings, Personal Data Sharing, Data Inference	2
12	Balance Security and Usability, Balance Privacy and Security, Build a Secure Internet	2
Final Exam (35%)		

Course Passing Requirements:

To pass the module, the student must attain an average of **at least 60%.**

Special Regulations:

- Late Assignments will **NOT** be accepted for any reason.
- Missing any exam without an **acceptable** excuse will result in **a zero grade** for that exam.
- There will be **NO** makeup quizzes.
- Academic **honesty**:
    - Individual assignments must be each student's own work.
    - Cheating will result an official university disciplinary review.