CS808 Computer Security Fundamentals

Dr Rosanne English

Rosanne.English@strath.ac.uk

LT1411

Office hours: Typically Tuesdays 150pm-250pm weeks 2-11 in LT1411

24/9/2024

You need to be registered and connected to eduroam for this to work

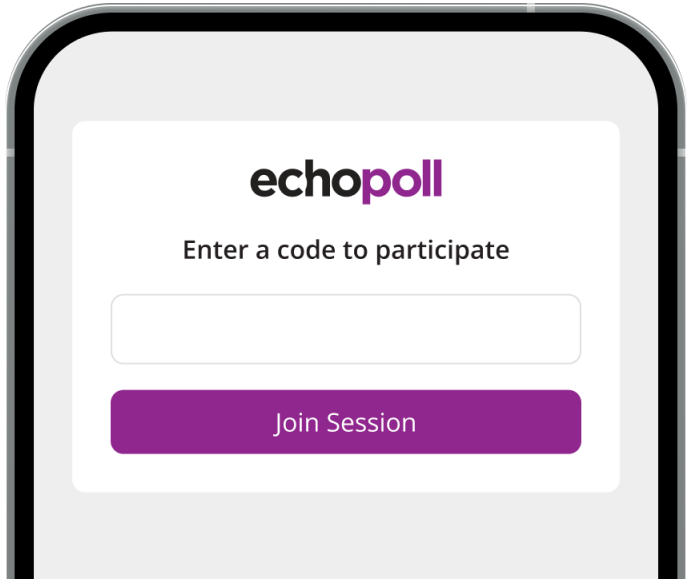
Scan the QR code below or use the password listed below to take your attendance

tq7oy8

To join the session

Go to

echo360poll.eu



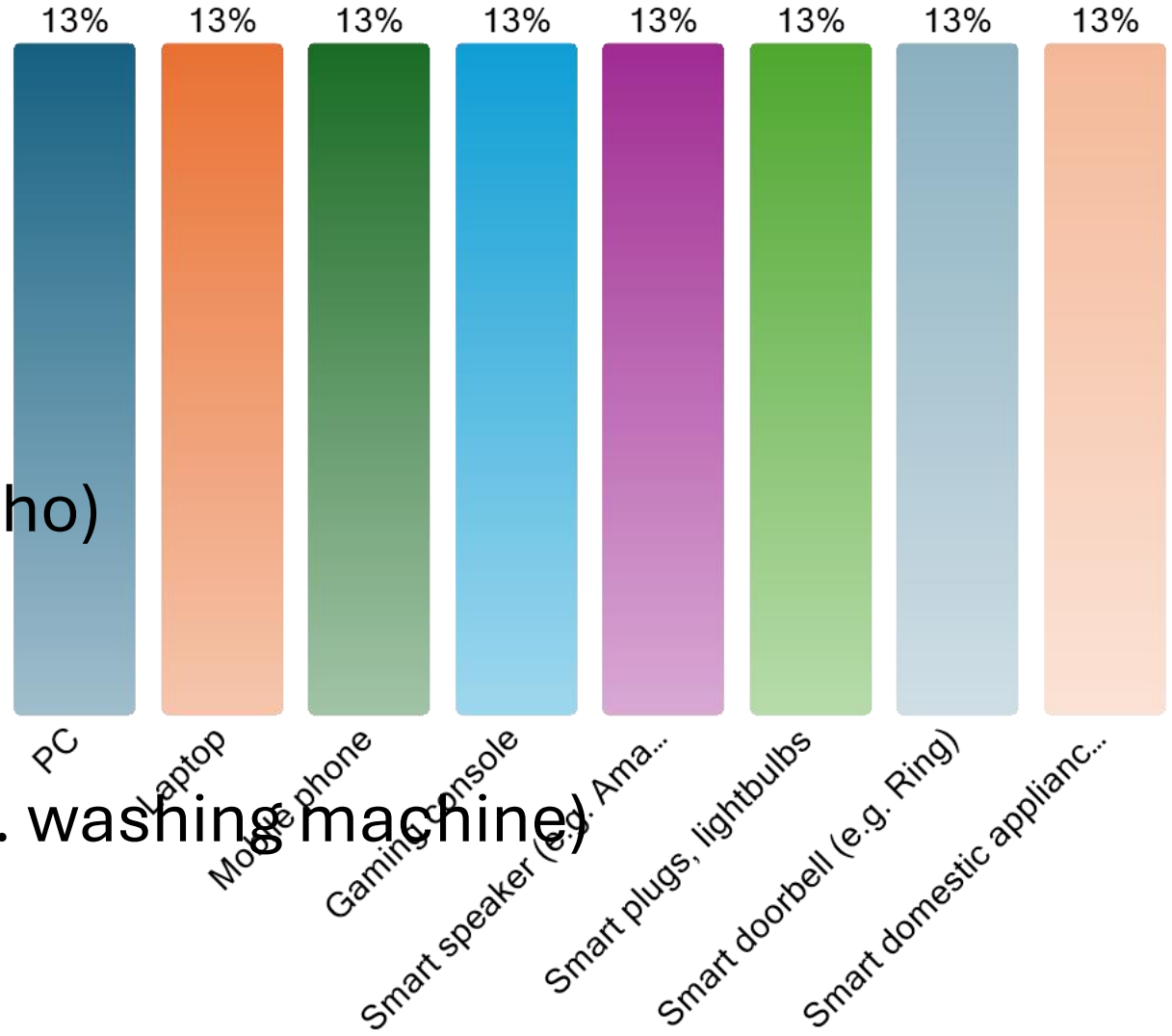
Enter code

3633364

Scan the QR code
with your device

Which of the following internet connected devices do you have in your home?

A. PC
B. Laptop
C. Mobile phone
D. Gaming console
E. Smart speaker (e.g. Amazon echo)
F. Smart plugs, lightbulbs
G. Smart doorbell (e.g. Ring)
H. Smart domestic appliance (e.g. washing machine)



The modern home…

Professional Cyber Qualifications

Certified Ethical Hacker
crypto, network sec, social engineering, malware, web sec

The CompTIA Security+ exam includes the following domains and topics:

- Threats, attacks and vulnerabilities: Analyze indicators of compromise and determine types of malware or compare and contrast types of attacks
- Identity and Access Management: Implement identity and access management controls or differentiate common account management practices
- Technologies and Tools: Troubleshoot common security issues or deploy mobile devices securely
- Risk Management: Explain the importance of policies, plans and procedures related to organizational security
- Architecture and Design: Summarize secure application development, deployment, cloud and virtualization concepts
- Cryptography and PKI: Compare and contrast basic concepts of cryptography or implement public key infrastructure

ISO 27K certification:
A.5: Information security policies (2 controls)
A.6: Organization of information security (7 controls)
A.7: Human resource security - 6 controls that are applied before, during, or after employment
A.8: Asset management (10 controls)
A.9: Access control (14 controls)
A.10: Cryptography (2 controls)
A.11: Physical and environmental security (15 controls)
A.12: Operations security (14 controls)
A.13: Communications security (7 controls)
A.14: System acquisition, development and maintenance (13 controls)
A.15: Supplier relationships (5 controls)
A.16: Information security incident management (7 controls)
A.17: Information security aspects of business continuity management (4 controls)
A.18: Compliance; with internal requirements, such as policies, and with external requirements, such as laws (8 controls)

Developing a Security Mind-set

Intended Learning Objectives

- Differentiate between secure communication solutions to determine an appropriate solution for a given context
- Evaluate an existing or proposed system in terms of potential security vulnerabilities and recommend the most appropriate security solution to apply
- Critique the security of a given network scenario
- Contribute to analysis of cyber risk and threat modelling

(Notional) Learning Hours

10 credits = 100 notional hours

- Pre- session activities: e.g. short educational videos, lab exercises, articles, attempt questions 20 hours (across 9 weeks)
- Contact hours: tutorial questions, guest speakers etc. 10 hours
- Self-study: including assessment 70 hours

Topics

Week 1: Welcome and Introducing Security

Week 2: Introduction to Cryptography

Week 3: Further Cryptography

Week 4: Steganography and User Authentication

Week 5: Malware

Week 6: Human Centred Security

Week 7: Network Attacks

Week 8: Network Defence

Week 9: Threat Analysis

Week 10: Assessed quiz

Week 11: NO CLASS (main coursework due)

Weekly Structure

- **Complete pre-lecture videos and activities** (typically no more than 2- 3 hours) *some weeks may be more, some less*
- ***Question sheets – Please attempt before coming to class***
- Add any questions to weekly forum
- Questions from forum and question sheets addressed in lecture sessions (Tuesday 3pm-4pm, GH713 except week 10, confirm through timetable)

(Typical) Tutorial Sessions

- first 10 minutes addressing questions from forum
- 15 minutes – comprehension quiz
- 25 minutes discussing scenario questions

Assessment Structure

- 30% - MyPlace quiz (individual, multiple choice)- assesses core understanding of material takes place in lab (LT501) on campus week 10
- 70% Individual Case Study – 4th December

Adjustments from Student Feedback

- Additional space for discussion after in class quiz
- Removal of exam – students found this challenging to manage in the timescale
- More slides in mini-lecture videos
- Lecturer written solution guides for questions, will appear following week
- More detail on some slides

Please let me know any feedback you might have, there will be a module evaluation at the end of semester but it's important to communicate concerns in advance

Ensure you read the module handbook and complete the academic integrity quiz

Academic Integrity

- Academic misconduct to present work which is not your own as work which is yours

Feedback in CS808

From me-

- Written: on coursework, responses to forums on MyPlace, email responses and notifications through MyPlace, quiz results
- Verbal: discussions in class, summary feedback on assessment, office hours discussions, responses to questions in tutorial session

From each other-

- discussions in class, responses to questions in tutorial session

Where to get help

1. Module handbook and myplace
2. Contact hours (Tues 3pm-4pm)
3. Book office hour appointment (Typically Tues 150pm-250pm weeks 2-11)
4. Email (include CS808 in subject header)