Get ready for MSc Cyber Security

Welcome to UWE Bristol. We are delighted that you have chosen to study MSc Cyber Security with us, and we very much look forward to meeting you on campus as you start your learning journey. As an Academic Centre of Excellence in Cyber Security Education (ACE-CSE), as certified by the UK National Cyber Security Centre, you will be conducting practical hands-on study to learn about the latest developments and technologies related to Cyber Security, including the nature of computer systems and networks, advances in how we manage and investigate data and devices, as well as operational aspects of security. As an advanced master's qualification, you will learn at pace and grasp new ideas to put these into practice, through interactive lab sessions and through self-study. We want you to succeed, and so this Preparing to Study letter is intended to guide you to a selection of activities that will have direct relevance on your successful study, as well as providing a flavour of what is to come when you join us at UWE Bristol.

Good luck in your future studies and we look forward to welcoming you to our university.

Abdullahi Arabo & Faiza Medjek
Programme Leader Team

Before you start

We are looking forward to welcoming you in the week commencing **20th January 2025** for Starting Block and the beginning of your programme.

Starting Block will help you settle into university and to help you get to know your teaching team and course mates. We will help you find your way around, get used to our systems, and practise the skills you need to make a strong start. Look out for further emails and explore the Starting Block website with more details.

Your timetable will be available to you via MYUWE (login required) once you have started the registration process. Please visit the 'Understanding your teaching timetable' website to find out when your timetable will be published.

Preparing and arrival

You can find everything you need to know about registration, Starting Block and the start of teaching, on our Preparing and Arrival webpage. Take a look at our website to familiarise yourself with our facilities and services such as the library, study skills, academic support, health and wellbeing support and much more.

Registration

Once you have satisfied all admissions requirements, we'll send you your login details for our IT systems to enable you to activate your university email account. Once your account has been activated, you'll gain access to the MYUWE platform where you can register. You can find guidance and further information on our Registration website.

ID card - upload your photo now

We can only print your ID card if you have added your photo to your MYUWE profile. Navigate to the 'My Details' tab where you can find ID Photo facility to upload a suitable photograph and receive your ID card without delay.

Engage with your programme

Start your learning

The following activities are designed to help you get started with the programme activities so that you can get the most out of your study. It is expected that you should be able to complete these activities before you start your programme, as successful completion of these tasks will enable you to progress well in your studies.

Activity 1: Coding

Core technical skills for this programme are built upon an understanding of programming, using the languages C and Python. You will also be using the Linux terminal extensively, and so developing your skills and understanding of these is essential. **We strongly recommend that all students complete the two interactive online tutorials** on **C Programming** **and** **Python Programming** for establishing fundamental knowledge that will be required for success on the programme.

As well as using the online tutorials, you should familiarise yourself with the Linux operating system, and also the process of creating your own Virtual Machine environments. As a UWE student, you will be able to download a VMware license free of charge when you begin your studies. For now, we recommend you experiment with creating virtual machines using freely-available tools, either using VMware Player or VirtualBox.

You should download two freely available operating systems, that we will use extensively during the course: Ubuntu Desktop and Kali Linux. You should use the downloaded ISO files to create a virtual machine within either VirtualBox or VMware Workstation Player (note that VMware Workstation Player will allow you to only create a single VM, VirtualBox allows you to create multiple VMs). Create two new virtual machines, one for Ubuntu and one for Kali, and install the respective operating systems.

If you have completed the earlier C programming tasks online, you should now try to create a standalone C program within Ubuntu. Create a new file called HelloWorld.c, and type the following code:

```
#include <stdio.h>
int main() {
    printf("Hello World!");
    return 0;
}
```

From the Terminal command line interface, execute the following command:

```
gcc HelloWorld.c -o HelloWorld.out
```

You should now be able to execute the program by executing the following command:

```
./HelloWorld.out
```

Having been able to compile and execute a simple C program on your virtual machine, experiment with the other sample programs available from the interactive online tutorial.

Activity 2: Computer and Network Security

As part of your preparation for the module, we would like you to complete two traffic analysis exercises from https://www.malware-traffic-analysis.net/ and https://share.netresec.com/s/S5ZG2cDKB9AbqwS.

For each exercise, **we ask that you prepare a maximum of 3 PowerPoint slides that highlight the key parts of the analysis for each case and summarises the attack**. This exercise will help you develop your skills in analysing network traffic, identifying malicious activity, and reporting your findings.

Please choose any two exercises from the Malware Traffic Analysis website and create your slides based on your analysis of the network traffic. Make sure to include relevant information such as IP addresses, domains, points of infection, and file names where applicable, and explain how you arrived at your conclusions.

This exercise will help you develop critical skills that you will need throughout the course and beyond and will **form part of your first assessment for this module.**

Activity 3: IoT Systems Security

Here are four short programming tasks that you should complete to help reaffirm your knowledge from the C programming tutorial. This will be a warmup activity in C programming. It will also allow you to get familiar with pseudo random number generation and distribution, which will be used in the summative assignment for the IoT Systems Security module.

Consider the following code that generates pseudo random numbers between 0 and 9:

```
int random_number = (int) (10.0*rand()/(RAND_MAX + 1.0));
```

Using this (please don't make any change), write a C program for each of the following tasks:

1. **Mean Test** – Write a C program that can generate 1000 random numbers and calculate the mean. The final output should give a result close to 4.5.
2. **Frequency Test** – Write a C program that can generate 10,000 random numbers. Use an array to count the occurrence of each digit (0 through to 9). The final output should show that the occurrence of each digit is close to 10%.
3. **Odd-Even Test** – As task 2, however this time divide the numbers into odd and even groups. The final output should show 50% in each group.
4. **Serial Test** - Write a C program that can generate 10,000 pairs of random numbers (e.g., 02, 14). Use an array to count the occurrence of pairs of digits (00 through to 99). The final output should show that the occurrence of each pair is close to 1%.

Activity 4: Digital Forensics for Cyber Security

Imaging in digital forensics is one of the first and most important steps of an investigation and ties into one of the four key principles of forensics. This activity will introduce you to FTK Imager, a Windows acquisition tool included in various forensics toolkits. The following link will guide you through the steps of creating a drive image using FTK Imager:

https://www.sans.org/blog/forensics-101-acquiring-an-image-with-ftk-imager/

Activity 5: Cyber Security Futures Emerging Trends and Challenges (CSF)

CSF is a research-driven, highly interesting module. Before you embark on the journey, let's warm up and peep into the research world.

Visit Google Scholar to complete the following task:

Search, read, understand, and critically analyse the following papers focusing on the topic "Intrusion Detection."

- A Survey of Intrusion Detection Techniques, 1993, TF Lunt, Computers & Security, Elsevier.
- A Survey of Intrusion Detection Systems, 2002, Douglas J. Brown, Bill Suckow, and Tianqiu Wang, Department of Computer Science, University of California, San Diego, San Diego, CA 92093, USA.
- Systematic literature review on intrusion detection systems: Research trends, algorithms, methods, datasets, and limitations, Melad Mohammed Issa, Mohammad Aljanabi*, and Hassan M. Muhialdeen, 2024, Journal of Intelligent Systems 2024; 33: 20230248.

1. The above papers are from three different decades but focus on the same topic. Why do you think research has been produced on the same topic since at least 1993, and how has the research evolved over the years?
2. In general, why do you think research is important? Create an imaginary world without research. What would it look like?
3. After using Google Scholar for a few days, identify your area of interest in cyber security research before you join us in CSF at our lovely UWE.
4. Finally! Find me (Sarfraz Brohi) in Google Scholar and identify my research interest.

Connect with others

We host a LinkedIn group called "MSc Cyber Security at UWE" that is designed for all prospective, current and alumni students to join. It is a great opportunity to hear from past and present students about their experiences and what they have gone on to achieve after their studies.

We also use Twitter where you can keep up to date with the wide range of activities taking place, and the events that our academics are engaged with. There are two feeds you may be interested in, one for the School of Computing and Creative Technologies @UWE_CSCT, and one for the UWEcyber Academic Centre of Excellence in Cyber Security Education @UWEcyber.

Be prepared

Access support

Check information on our Disability webpages so you know what actions you need to take. Contact Disability Service and myself to let us know if you need any additional mobility or other support to fully access all activities during your studies.

Get equipped

The University provides computers on all our campuses for you to use in your studies. These computers will provide access to our core digital education tools and any specialist software required for your course. You may have scheduled sessions in computer labs or other specialist facilities, and you will be able to use open-access PCs for self-study.

The university licenses many specialist software packages for use on personal laptops for the duration of your course. The core software used in your course may include Blackboard, Collaborate, Panopto, Microsoft 365 (formerly Office 365), PebblePad, SPSS.
These packages will run on Windows devices but not on tablets or Chromebooks.

As a minimum specification for this programme, we would expect you to have access to an **Enhanced Specification** device. The **Intensive Specification is recommended** due to the nature of computer programming and virtual machine deployment. Please UWE website for detailed information on choosing your IT equipment including recommended specifications.

International students

The Global Student Support Team offer information and advice to ensure you receive all the support you need to get the best from your time at UWE Bristol. They are here to help you to settle in when you first arrive at UWE Bristol and organise social events to help you to adapt to your new environment.

Next steps

Before you arrive, you will receive an online workbook to introduce you to the School and help you to prepare for university life. You can go through the workbook then, and it will be revisited during your induction activities.

Who to contact if you have questions

For any questions about the programme, please contact me, **Abdullahi Arabo** via email at abdullahi.arabo@uwe.ac.uk.

Please note: this information has been provided on the assumption that you will meet the conditions of your offer and be eligible to take up your place.

Entry: January 2025 Last updated: October 2024