CyberFirst **Defenders**

CyberFirst Defenders aims to inspire and excite pupils about cyber security. It is designed for 14 - 15 year old pupils with a demonstrable interest in computing and provides them with a valuable introduction to all the tools, knowledge and skills cyberists need to build and protect small networks and personal devices. It complements the GCSE computing curriculum and takes it a step further, offering practical methods to help protect and secure everyday devices, apps and software.

Module content consists of interactive, hands on, self-guided, exploratory learning. Reducing the amount of time spent in traditional instructor led presentations to the very minimum.

Day 1 - Insecure by Default

This day focuses on introducing the students to the Internet of Things and developing their understanding of the evolution of the internet and its use. Students are encouraged to build their own team network.

Day 2 - Securing your Devices

The focus of this day is on developing an understanding of good practice for securing common devices. Students practice their new found knowledge by breaking, fixing and securing the devices on their team network.

Day 3 - Understanding Networks

In this module we look at the wide variety of attackers; who are they and what are their motivations?

Day 4 - Securing Yourself

The operating system is the interface between the user and the device, making it a valuable target to attackers. In this module we explore how the operating system can be attacked and secured.

Day 5 - Securing Your Loved Ones

Attendees will leave the course equipped with practical knowledge that they will need to help protect their friends and family.

Course **Overview**

CyberFirst Defenders events are designed to introduce 14 to 15 year-olds to the tools, knowledge and skills required to pursue a career in the field of cyber security.
It builds upon the computer science GCSE to provide students with the practical skills that they require to protect themselves, their friends and their families online by securing everyday devices, home networks and commonly used apps and software.

Our CyberFirst Defenders courses run for 5 days between 09:00 and 17:00 and are delivered by subject matter experts, as well as guests from industry and academia.

Each event consists of 12 modules offering interactive, hands on, self-guided, exploratory learning.

Training **Goals**

- To encourage school pupils who are already studying computer science at GCSE level to continue to study the subject at A Level
- To encourage school pupils who are not studying computer science or related STEM subjects at GCSE level to study the subjects at A Level.
- To encourage school pupils to pursue a career in cyber security.
- To identify talented pupils who may be eligible for the CyberFirst bursary in the future.

Learning **Objectives**

During the CyberFirst Defenders course attendees will:

- Explore modern home devices; how to connect them and protect them
- Understand modern IoT devices and the security challenges that the Internet of Things poses
- Discover the vulnerabilities that threaten your apps, your home network and your personal devices
- Understand modern operating systems
- Become more security aware; learn how to protect yourself, your devices and your home network using user accounts, good passphrase practice, multifactor authentication and encryption.
- Understand how networks work and get hands-on experience of creating and protecting a home network
- Protect yourself and your personal data
- Hear from inspirational speakers about the range of careers that are available in the field of cyber security
- Learn from subject matter experts how cyber security skills can improve your career prospects
- Work in diverse teams to tackle exciting hands-on challenges
- Learn about the legal and ethical decisions which concern cyberists

Course **Outline**

Module 1 - The Internet of Things

Developments in sensor technology have led to an incredible rise in the number of Internet connected "Things". These inexpensive, low powered and always on smart devices form the Internet of Things. In this module we look at what the IoT is, how it is used and what affect it will have on the businesses, cities and individuals of the future.

Module 2 - Security in the Internet of Things

In this module we consider the privacy and security concerns around IoT devices and how the IoT can be attacked and secured.

Module 3 - How do Attackers Attack?

In this module we look at the wide variety of attackers; who are they and what are their motivations?

Module 5 - Passwords

We use passwords to protect all of our online accounts. In this module we look at how passwords work, what makes a strong password and how attackers obtain and break them.

Module 6 - Data Security

In this module we use different encryption methods, user profiles, permissions and file systems to protect valuable personal data.

Module 7 - Apps and Malware

In this module we investigate the difference between legal and illegal software and explore the consequences of using software from unknown sources. We look at how malware works and how it can be stopped through good cyber hygiene practices.

Module 8 - Networks

This module provides students with an understanding of what networks are and how they work. Students will learn about the fundamentals of Ethernet and WiFi networks as well as develop an understanding of the core protocols in the TCP/IP suite.

Module 9 - The TCP / IP Protocol Suite

In this module we introduce the protocols that enable networks and the internet.

Module 10 - Transport Protocols

In this module we look at how network communications work and how they can be secured and intercepted.

Module 11 - Using the Internet

In this module we look at the technologies that leverage network communications, the languages that are used and the security implications of cookies, metadata and fraudulent websites.

Module 12 - Social Media

In this module we help students to understand how using social media and web sites can expose personal information about them to third parties and what steps they can take to limit their digital footprint and avoid online fraud.